**UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

| | |
|---|---|
| KENNETH HASSON, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>COMCAST CABLE COMMUNICATIONS LLC, COMCAST CORPORATION, CITRIX SYSTEMS, INC., and CLOUD SOFTWARE GROUP, INC.,<br><br>Defendants.<br><br>This Document Relates to: All Actions | Master File No. 2:23-cv-05039-JMY |

**PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS**

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

**Cases**

**Statutes**

**Rules**



**Other Authorities**

Comcast makes an audacious ask of this Court: to forgo procedural safeguards and decide questions of merit at the pleading stage. Although disguised as a "jurisdictional challenge," Comcast argues Plaintiffs were not harmed by it because the compromised data was not sensitive. Comcast is wrong. Plaintiffs' compromised data, including full names, billing/residential addresses, usernames, crackable hashed passwords, secret questions and answers, and partial social security numbers, is indeed sensitive, and Plaintiffs were injured when this sensitive data was exposed to unauthorized third parties through Defendants' poor data security measures. However characterized, Comcast's argument is a direct attack on the merits of Plaintiffs' claims. Whether rooted in tort, contract, or statute, each claim requires Plaintiffs to show that they suffered injury caused by Defendants. This requires Plaintiffs to build a record as to, for example, what data was compromised, how risky that data is, and whether harm occurred or will occur. At a minimum, these issues impact the duty, breach, causation, and injury/damages elements of Plaintiffs' claims. Comcast's current motion would strip Plaintiffs of their right and ability to develop this record *at the pleading stage*. This violates binding Third Circuit precedent. *See Davis v. Wells Fargo*, 824 F.3d 333, 348–49 (3d Cir. 2016) (reversing trial court on standing and cautioning against courts "allowing a Rule 12(b)(1) motion to dismiss for lack of subject matter jurisdiction to be turned into an attack on the merits."). Comcast's motion is procedurally improper.

Remarkably, Comcast bases its brazen factual attack on two meager declarations. The crux of Comcast's argument is that Plaintiffs were not injured because they only had certain, non-sensitive data stored in Comcast's records ("Enterprise Service Directory," or "ESD") that was not posted on the dark web. Defendants support this argument with a *two-page* declaration from Sandra Cavazos and a *two-page* declaration from Adam Darrah. These self-serving, conclusory, and unfounded declarations lack credibility and are inadmissible. For example, though Cavazos

claims Comcast created a "forensic copy" containing the scope of Plaintiffs' data available to threat actors, Cavazos does not explain Comcast's methodology for creating the forensic copy or how it could create a forensic copy almost a month after the Data Breach. Indeed, a "forensic copy" is an industry standard term, and when such a copy is created improperly—whether through shortcuts, failure to follow industry standard methods, or otherwise—it can lead to an unreliable final result. Nor does she describe what changes the "constantly changing" ESD underwent in the interim. Thus, Comcast's argument depends entirely on the accuracy of a "forensic copy" made nearly a month after the Data Breach, with ***zero*** explanation of how that copy was created, preserved, or authenticated. And Darrah's contention that Plaintiffs' data is not available on the sites identified by Plaintiffs' First Amended Consolidated Complaint ("FACC") is based entirely on hearsay that Darrah himself does not have the requisite training, education, or experience to confirm or rely. These declarations should be stricken or, at the very least, disregarded.[1]

Comcast also relies on unreliable *attorney argument* to state that no third party "was able to or could derive a Plaintiff's actual password from a hashed password." ECF No. 158-2, at 20. But Comcast provides no affidavit, declaration, or sworn testimony from any purported expert about Comcast's hashing algorithm. It does not because it cannot. For if Comcast provided this evidence, it would have to reveal that its insecure password hashing algorithm is vulnerable and easily decipherable. Indeed, in limited testing, Plaintiffs' expert was able to crack the hashed passwords for several Plaintiffs using tools and techniques commonly employed by cybercriminals, such as rainbow tables, look up tables, and brute force methods. *See* Declaration of Matthew Strebe ¶¶ 18-20, attached as Exhibit A. The hashed passwords are not "innocuous" as

[1] Plaintiffs have simultaneously filed a motion to strike the declarations of Sandra Cavazos and Adam Darrah.

Comcast claims—quite the opposite, actually.

Despite Comcast's efforts to deny Plaintiffs access to this Court, Plaintiffs conclusively establish Article III standing. Comcast's factual challenge rests solely on those two declarations and attorney argument that, as more fully explained in Part III, are both unreliable and inadequate. In contrast, Plaintiffs submit detailed declarations from qualified experts that affirmatively establish Article III standing. As previewed above, Matthew Strebe, the Chief Information Security Officer and Founder of an IT consulting firm, refutes Comcast's assertion that its data analysis of ESD is definitive and establishes that the exposed hashed passwords are, in fact, vulnerable and insecure. *See* Ex. A, Strebe Decl. David Nelson, a cybercrime investigator with about 20 years of experience with the cybercrime division of the FBI, explains that Plaintiffs' PII appeared on the dark web shortly after the breach, and that this temporal proximity—coupled with instances of fraud experienced by several Plaintiffs—strongly supports a causal connection. *See* Declaration of David Nelson, attached as Exhibit B. And Matthew O'Neill, a former Deputy Special Agent of Cyber Operations, Criminal Investigative Division of the U.S. Secret Service, further confirms standing by detailing the sensitive nature of Plaintiffs' compromised data, the substantial and imminent risks to Plaintiffs posed by its exposure, and the traceability of identity theft and fraud suffered by Plaintiffs from the Data Breach itself. *See* Declaration of Matthew O'Neill, attached as Exhibit C. In a data breach like this where cybercriminals successfully targeted customer sensitive data by exploiting Citrix's prematurely disclosed vulnerability and traversing Comcast's inadequate data security, Plaintiffs have met their burden for Article III standing.

Citrix's motion follows the same fate. Instead of a factual attack, Citrix makes a facial one. But facially, Plaintiffs have adequately pled how their injuries are traceable to Citrix's failures related to the Data Breach. And Citrix's improper distortion of traceability principles is insufficient

to disrupt this link. Similarly, Citrix's other attempt to escape liability under Rule 12(b)(6) is futile. Plaintiffs are not asking the Court to create a new duty. Rather, Plaintiffs are simply asking the Court to apply settled tort principles to the facts here. Citrix cannot hide from the fact that its irresponsible disclosure alerted the world (including cybercriminals) to the existence of a critical vulnerability in its products *before* providing customers like Comcast with complete mitigation guidance. And as a result of Citrix's irresponsible disclosure, threat attackers targeted Comcast and its customer data. Citrix predicted this risk and thought it significant enough to include in its 2021 10-K Annual Report. It is disingenuous now for Citrix to argue Plaintiffs' and the Classes' injuries were not foreseeable.

Ultimately, Defendants' requested relief is unattainable. Their motions do not strip this Court of its authority to hear Plaintiffs' claims, nor do they provide Defendants with a path to an early exit from this litigation. Accordingly, this Court should deny Defendants' motions to dismiss.

## STATEMENT OF FACTS

Comcast is one of the largest companies in the telecommunications sector. FACC ¶ 1. It provides internet services and products, cable television, a mobile 5G network, and landline telephone services across the country under the brand name Xfinity. *Id.* Similarly, Citrix is one of the largest companies in the office technology sector. *Id.* ¶ 2. Citrix provides an array of business technology services like server, application, and desktop virtualization, networking, Software-as-a-Service, and cloud computing to hundreds of thousands of clients worldwide. *Id.* Comcast contracted with Citrix to provide a variety of networking hardware and software services, including Citrix's NetScaler ADC and NetScaler Gateway (the "NetScaler Products"). *Id.* The NetScaler Products purportedly improve the efficiency and speeds of applications and consolidate remote access infrastructure by providing a single-sign-on across all applications. *Id.* ¶ 209. Put

simply, it allows a Comcast user to access any application, from any device, through a single URL.

Defendants' business models require they store, use, and transfer sensitive and private customer information or at least provide access to such information. *Id.* ¶¶ 3, 183-224. For example, Comcast requires customers to provide private and sensitive information for its products and services, including name, phone number, residential address, date of birth, Social Security numbers, demographic information, and so on. *Id.* ¶ 188. According to Comcast, this information allows it to improve its services, develop new products and services, give recommendations, deliver personalized consumer experiences (including marketing and advertising for its own and others' products and services), investigate theft and illegal activities, and to ensure a secure online environment. *Id.* ¶¶ 343-348.

Given the nature of information they possess and provide access to, Defendants make several promises and representations about their cybersecurity. For example, Comcast recognizes its duty to safeguard its customers' PII: "[w]e don't expect our customers to be cybersecurity experts. That's why we make a point of prioritizing security for them, from the gateway in their home through to the core of our network."[2] And that Comcast "follow[s] industry-standard practices to secure the information we collect to prevent unauthorized access, use, or disclosure of any personal information we collect and maintain." *Id.* ¶ 196. Citrix also recognizes that its products may be used to provide access to sensitive customer information like Plaintiffs' PII. For instance, [redacted]

[2] Noopur Davis, *Noopur Davis: Secure Customers are What Matter Most*, COMCAST, https://corporate.comcast.com/stories/noopur-davis-secure-customers-are-what-matter-most (last visited Apr. 30, 2025). This quote is from a link in footnote 1 on the caption page to the FACC that was inadvertently omitted from the filing.

[redacted] Furthermore, in its 2021 10-K Annual Report, Citrix states that unauthorized parties may attempt to compromise confidential information of its customers or their end users and that this may result in individual and/or class action lawsuit. *Id.* ¶ 215.

On October 10, 2023, Citrix published a security bulletin entitled "NetScalerADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967" that announced: "Multiple vulnerabilities have been discovered in [the NetScaler Products]." *Id.* ¶ 281. The CVE-2023-4966 vulnerability ("Citrix Bleed") allows cybercriminals to gain unauthorized access to sensitive data contained in a vulnerable system. *Id.* ¶ 283. Specifically, a cybercriminal exploiting Citrix Bleed sends a specially crafted HTTP GET request to a vulnerable NetScaler appliance (like the NetScaler Products), which returns a session cookie that allows the hacker to establish an authenticated session in the NetScaler appliance without any need for a username, password, or multi-factor authentication ("MFA"). *Id.* In other words, cybercriminals exploiting Citrix Bleed hijacked legitimate users' already-active sessions. *Id.* This security bulletin included a "patch" that customers like Comcast could install to patch the vulnerability. *Id.* Citrix recommended that its customer using the NetScaler Products should "install the relevant updated versions" of the software "as soon as possible." *Id.* ¶ 309. But although Citrix first published this patch and guidance on October 10, 2023, exploitation of Citrix Bleed had already been ongoing for the two months, apparently unnoticed by Citrix. *Id.* ¶ 306. This means that Citrix was not adequately monitoring its NetScaler Products for vulnerabilities, despite this being industry standard. *Id.* ¶ 341.

Like Citrix, Comcast also waited too long to act. Despite receiving the patch and guidance on October 10, 2023, Comcast did not implement the patch until over a week later. *Id.* ¶ 285. Comcast's decision to finally implement the patch likely had to do with Citrix's updated guidance released on October 17, 2023, that "**[e]xploits of CVE-2023-4966 on unmitigated appliances have been observed.**" *Id.* ¶ 309. Then six days after, Citrix again provided more guidance recommending that those using the NetScaler Products "kill[ ] all active and persistent sessions[.]" *Id.* This additional advice should have been provided in its earlier guidance.

Citrix's insufficient and untimely guidance coupled with Comcast's delay proved catastrophic. Comcast later discovered that—during its delay in implementing the patch—cybercriminals hacked into its systems by exploiting Citrix Bleed. *Id.* ¶ 314. Specifically, between October 16 and October 19, 2023, cybercriminals gained unauthorized access to Comcast's internal systems and acquired usernames and passwords, names, contact information, last four digits of Social Security numbers, dates of birth and/or secret questions and answers ("PII") for nearly 36 million former and current Comcast customers (the "Data Breach"). *Id.* ¶¶ 314-318. Had Citrix adequately tested and monitored its NetScaler Products, timely provided complete and accurate guidance about Citrix Bleed and the patch, and actually distributed the patch before public disclosure of the vulnerability, the Data Breach could have been mitigated or avoided altogether. *Id.* ¶¶ 8-9, 312-13, 485. Similarly, the Data Breach could have also been mitigated had Comcast heeded Citrix's instruction to install the patch "as soon as possible." *Id.* ¶¶ 5, 269. Both Defendants are blameworthy.

More than two months after the Data Breach, Comcast finally disclosed to Plaintiffs that it experienced a data breach. *Id.* ¶ 314. But this notice was lacking. The notice provided minimal information that an unauthorized party acquired PII for its customers. *Id.* The notice did not explain

how hackers stole customers' PII, when Comcast actually patched its system, or who was responsible for the Data Breach. *See generally id.* Comcast did not offer credit monitoring services to most of its customers. *Id.* But Comcast simultaneously acknowledged the risk posed to its customers because of the Data Breach, "strongly encourag[ing]" them to enroll in MFA and directing them to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports." *Id.* Comcast then supplemented its notice a month later. *Id.* In its supplemental notice, Comcast revealed that full Social Security numbers and/or driver's license numbers were also acquired for a portion of its customers during the Data Breach. *Id.* Based on Comcast's notices, certain PII—including Social Security numbers, driver's license numbers, and secret questions and answers—was not encrypted, despite encryption of sensitive information being industry standard.

Unfortunately for Plaintiffs and Class Members, Comcast was right that victims needed to "remain vigilant." Following the Data Breach, cybercriminals offered Plaintiffs' stolen PII for sale on the Dark Web. *Id.* ¶ 350; *see also* Ex.B, Nelson Decl. The Dark Web is a heavily encrypted part of the Internet that conceals users' identities and online activity, making it difficult for authorities to detect the location or owners of a website when illegally-acquired information is disclosed or put up for sale. FACC ¶¶ 200, 350; Ex. B, Nelson Decl. ¶ 4 n.1. Furthermore, multiple sets of Comcast/Xfinity data were uploaded to a Torrent site called "Fox Store" where cybercriminals sell and purchase PII. FACC ¶ 350; Ex. B, Nelson Decl. ¶¶ 8-9. This data was uploaded on October 16, 2023 and October 23, 2023—the first day and one week after the Data Breach. *Id.* During that same month, a post titled "700K Comcast.net private combolist" was posted onto the Dark Web. Ex. B., Nelson Decl. ¶ 10. And in July 2024, additional sets of data were posted on Niflheim World-Black Bet. Ex. B., Nelson Decl. ¶ 8. Furthermore, the pervasive fraud and identity theft

experienced by Plaintiffs and Class Members indicate their information is already circulating for sale on the Dark Web. Given the temporal proximity of the uploads of the Xfinity data to the Data Breach and the specific allegations of fraud and identity theft, it is highly likely Plaintiffs' PII was part of this data. Ex. B, Nelson Decl. ¶¶ 12-13.

As a result of Comcast's and Citrix's inadequate security measures, Plaintiffs have suffered injury and face an imminent and substantial risk of further injury, including identity theft and related cybercrimes. *See* FACC ¶¶ 349-363 (detailing wide-ranging impact of data breach on plaintiffs); *see also* Ex. C, O'Neill Decl. In addition, as a result of the Data Breach, Named Plaintiffs have experienced severe and pervasive fraud and identity theft; spent time and money dealing with attempted fraud and identity theft; and expended resources, including time, protecting themselves against fraud and identity theft. *See, e.g.*, FACC ¶¶ 13-24; Andros Decl. ¶ 11, attached as Exhibit G (Andros: fraudulent charges appearing on her debit card); ¶¶ 25-37; Birnie Decl. ¶ 9, attached as Exhibit H (Birnie: fraudulent charges using her credit card, attempts to access her other accounts, costs to replace special photo on debit card); ¶¶ 38-50; Durham Decl. ¶ 11, attached as Exhibit I (Durham: fraudulent withdrawal of money from bank account); ¶¶ 51-65; Estevez Decl. ¶¶ 12-14, attached as Exhibit J (Estevez: fell victim to port-out fraud where cybercriminals highjacked his phone and gained access to his financial accounts); ¶¶ 66-77; Fail Decl. ¶ 11, attached as Exhibit K (Fail: unauthorized charges on bank statement); ¶¶ 90-101; Nanez Decl. ¶ 10, attached as Exhibit M (Nanez: attempted access on a different account used by her minor son); Prescott Decl. ¶ 11, attached as Exhibit O (Prescott: several fraudulent Zelle charges); ¶¶ 125-138; Smith Decl. ¶ 7, attached as Exhibit P (Smith: a stranger attempted to open a Chase Bank account in Plaintiff Smith's name using the same PII compromised in the breach and victim of targeted phishing and social engineering attack); *see also* Ex. C, O'Neill Decl. ¶ 7. Facing a significant

present and ongoing risk of identity theft and related fraud, Plaintiffs will need to take measures indefinitely to protect themselves as a result of the data breach. FACC ¶¶ 349-363; Ex. C, O'Neill Decl. ¶¶ 26-27.

As explained fully below, Plaintiffs' allegations are factually and facially plausible. Defendants' motions to dismiss should be denied in their entirety.

## LEGAL STANDARDS

### I. RULE 12(B)(6) MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM.

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal,* 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly,* 550 U.S. 544, 570 (2007)). "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* Accordingly, a "claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Twombly,* 550 U.S. 544, 556 (2007). "In considering a motion to dismiss under Rule 12(b)(6), the Court 'accept[s] all factual allegations as true [and] construe[s] the complaint in the light most favorable to the plaintiff." *Est. of Rennick v. Universal Credit Serves., LLC,* No. CV 18-3881, 2019 WL 196539, at *2 (E.D. Pa. Jan. 15, 2019) (quoting *Warren Gen. Hosp. v. Amgen, Inc.,* 643 F.3d 77, 84 (3d Cir. 2011)). Only Citrix moves to dismiss under Rule 12(b)(6).

### II. RULE 12(B)(1) MOTION TO DISMISS FOR LACK OF SUBJECT MATTER JURISDICTION.

Under Article III of the United States Constitution, a federal court may decide only cases and controversies. *Const. Party of Pennsylvania v. Aichele*, 757 F.3d 347, 357 (3d Cir. 2014). This requires Article III standing. *Id.* (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)).

A challenge to Article III standing under Rule 12(b)(1) may be facial or factual. *Davis*, 824 F.3d at 346. A facial attack challenges subject matter jurisdiction "without disputing the facts alleged in the complaint," and it requires the Court to "consider the allegations of the complaint as true." *Id.* Thus, a facial attack under 12(b)(1) retains the same legal safeguards as a motion to dismiss under Rule 12(b)(6). *Const. Party of Pennsylvania*, 757 F.3d at 358.

A factual attack is different. A factual attack allows a party to challenge the complaint's assertion of jurisdiction through filing an answer or—as Comcast attempts here—presenting competing facts. *Davis*, 824 F.3d at 346. If there are competing facts, then the Court is "free to weigh the evidence and satisfy itself as to the existence of its power to hear the case." *Id*. But those competing facts must be in the form of admissible and competent evidence. *See Schuchardt v. President of United States*, 802 F. App'x 69, 74 (3d Cir. 2020). If there is no admissible and competent evidence, then there is nothing to controvert Plaintiffs' allegations. *Const. Party of Pennsylvania*, 757 F.3d at 358-59. And if Plaintiffs' allegations are uncontroverted, there is no factual dispute. *Id*. So, without a factual dispute, a factual attack devolves into a facial one. *Id.* Nonetheless, a factual attack "is inappropriate when the jurisdictional issue and substantive issues are so intertwined that the question of jurisdiction is dependent on the resolution of factual issues going to the merits of an action." *Davis*, 824 F.3d at 348. In this setting, "the proper procedure for the district court is to find that jurisdiction exists and deal with the objection as a direct attack on the merits of the plaintiff's case." *Id.*

## ARGUMENT

Citrix brings a facial attack on Article III standing, while Comcast brings a factual one. As a threshold matter, because Comcast's factual challenge is a direct attack on the merits of Plaintiffs' claims, the Court must "find that jurisdiction exists" and deny Comcast's motion. But

even if the Court does not deny on this basis, Defendants' motions to dismiss still fail. Because Comcast is relying on inadmissible evidence, it cannot controvert Plaintiffs' well-plead allegations. So Comcast's factual attack should be treated as facial one, like Citrix's. Facially, Plaintiffs plausibly allege how they were injured when their sensitive PII, such as their full names, billing/residential addresses, usernames, crackable hashed passwords, secret questions and answers, and partial social security numbers, was exposed to unauthorized third parties. And Plaintiffs' plausibly trace their instances of fraud and identity theft and the imminent and substantial risk of fraud and identity theft to Defendants' poor data security and business practices, which led Plaintiffs PII to be exposed in the first instance. Thus, when construing Plaintiffs' allegations in their favor and the complaint in the light most favorable to them, Plaintiffs have met their burden to show that they have Article III standing and may proceed in federal court. In fact, Defendants recognize that Plaintiffs plausibly plead Article III standing as they removed state court actions based on the same allegations. *See Fidelity & Deposit Co. of Md. v. Hudson United Bank*, 653 F.2d 766, 777 (3d Cir. 1981). Accordingly, Defendants' motions to dismiss should be denied.

## I. THE THIRD CIRCUIT CAUTIONS AGAINST FACTUAL ATTACKS ON ARTICLE III STANDING UNDER RULE 12(B)(1).

Defendants invite this Court to stray from binding precedent. The Third Circuit has "repeatedly cautioned against allowing a Rule 12(b)(1) motion to dismiss for lack of subject matter jurisdiction to be turned into an attack on the merits." *Davis*, 824 F.3d at 348 (collecting cases, and vacating district court's order granting 12(b)(1) attack on standing). Only in "narrow categories of cases" may courts dismiss under Rule 12(b)(1) for merits-related defects—namely, "where the alleged claim under the Constitution or federal statutes clearly appears to be immaterial . . . or where such a claim is wholly insubstantial and frivolous." *Id.* at 350 (quoting *Bell v. Hood*, 327 U.S. 678, 682-83 (1946)). Even in the rare case that a court may consider a disputed factual issue

that goes both to the merits and jurisdiction, "district courts must 'demand less in the way of jurisdictional proof than would be appropriate at a trial stage.'" *Davis*, 824 F.3d at 350 (quoting *Mortensen v. First Fed. Sav. & Loan Ass'n*, 549 F.2d 884, 892 (3d Cir. 1977)). But such circumstances are rare, and the Third Circuit has repeatedly emphasized that "Rule 12(b)(1) must not be expanded beyond its proper purpose." *Davis*, 824 F.3d at 349.

This caution is for good reason. Granting a motion to dismiss under these circumstances strips the judicial process of its legal safeguards and flips the burden of persuasion on its head:

> Caution is necessary because the standards governing the two rules differ markedly, as Rule 12(b)(6) provides greater procedural safeguards for plaintiffs than does Rule 12(b)(1). First, proceeding under Rule 12(b)(1) inverts the burden of persuasion. When presenting a Rule 12(b)(6) motion, the defendant bears the burden to show that the plaintiff has not stated a claim. *Kehr Packages*, 926 F.2d at 1409. But under Rule 12(b)(1), the plaintiff must prove the court has subject matter jurisdiction. *Id.* The two rules also treat the complaint's factual allegations very differently. Unlike Rule 12(b)(6), under which a defendant cannot contest the plaintiff's factual allegations, Rule 12(b)(1) allows a defendant to attack the allegations in the complaint and submit contrary evidence in its effort to show that the court lacks jurisdiction. *Mortensen*, 549 F.2d at 891. Thus, improper consideration of a merits question under Rule 12(b)(1) significantly raises both the factual and legal burden on the plaintiff. Given the differences between the two rules, "[a] plaintiff may be prejudiced if what is, in essence, a Rule 12(b)(6) challenge to the complaint is treated as a Rule 12(b)(1) motion." *Kehr Packages*, 926 F.2d at 1409.

*Davis*, 824 F.3d at 348–49. Because of its "procedural and substantive protections for plaintiffs," Rule 12(b)(6) "is the proper vehicle for the early testing of a plaintiff's claims." *Id.*

Thus, on a 12(b)(1) motion, a court must "carefully separate [the] standing inquiry from any assessment of the merits of the plaintiff's claim." *Adam v. Barone*, 41 F.4th 230, 234 (3d Cir. 2022). Because the risk of erroneously conflating standing and the merits is particularly acute in a factual challenge to standing, "dismissal via a Rule 12(b)(1) factual challenge to standing should be granted sparingly." *Davis*, 824 F.3d at 350; *see also Hartig Drug Co. Inc. v. Senju Pharm. Co.*, 836 F.3d 261, 273 (3d Cir. 2016) (citation omitted) (stating that "dismissal via a Rule 12(b)(1)

factual challenge to standing should be granted sparingly, and it is only the 'unusual' case that will be properly dismissed under 12(b)(1)").

## II. DEFENDANTS' PURPORTED JURISDICTIONAL CONCERNS ARE A DIRECT ATTACK ON THE MERITS OF THE CASE.

Comcast's "jurisdictional" motion improperly conflates jurisdictional arguments with merits arguments. In support of its motion, Comcast argues that Plaintiffs' data is not in the hands of criminals nor on the dark web, that Plaintiffs' data is not sensitive, and that Plaintiffs lack any cognizable damages caused by Defendants. *See generally* ECF No. 158-2. These arguments directly challenge Plaintiffs' claims, which would typically be addressed at summary judgment or trial on a fully developed record. For example, any duties or obligations that Defendants may have to Plaintiffs and any breach of those duties or obligations depend on the nature, scope, and sensitivity of Plaintiffs' data.

Courts regularly reject this type of disguised merits attack in data breach cases. *See, e.g. In re Blackbaud, Inc., Customer Data Breach Litig.,* No. 3:20-MN-02972-JMC, 2021 WL 2718439, at *5 (D.S.C. July 1, 2021) (refusing to entertain factual attack on plaintiffs' standing in data breach case, because the "factual challenge to . . . Article III standing involve[d] facts that are intertwined with the merits of Plaintiffs' claims[.]"); *In re Mednax Services, Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1207 (S.D. Fla. 2022) ("Defendants' contentions are indirect, if not direct, attacks on the merits of Plaintiffs' case. As such, those questions must be resolved at the summary judgment stage after both parties have had an opportunity to develop the record through discovery."); *Allgood v. PaperlessPay Corp*., No. 3:20-CV-516, 2022 WL 846070, at *9 (M.D. Fla. Mar. 22, 2022) (rejecting 12(b)(1) factual attack on plaintiffs' causation and damages allegations in data breach case as "a direct attack on the merits of the case" that was "premature"); *Salas v. Acuity-CHS, LLC*, No. 22-cv-317-RGA, 2023 WL 2710180, at *3 (D. Del. Mar. 30, 2023)

(denying 12(b)(1) motion in data breach case based on imminence and concreteness of plaintiff's injuries, and noting that courts "must take care not to conflate the standing inquiry with an assessment of the merits of [p]laintiff's claim"). Courts consistently reject this tactic in other contexts as well. *See, e.g.*, *Okeke v. LNL Home Services, LLC*, No. 21-cv-4705, 2022 WL 1017618, at *2 (E.D. Pa. Apr. 5, 2022) (denying 12(b)(1) motion that disputed allegations in complaint).[3] The Court should not countenance this practice.

Comcast relies on a handful of decisions outside this circuit that do not reflect the realities here nor Third Circuit jurisprudence. For example, in *Cantinieri v. Verisk Analytics, Inc.*, No. 21-CV-6911 (NJC) (JMW), 2024 WL 5202579 (E.D.N.Y. Dec. 23, 2024), the plaintiff proffered no evidence (through expert or otherwise) to show how hackers' access to the portal could provide access to the Social Security number to result in fraud. Similarly, in *Foster v. Essex Prop., Inc.*, No. 5:14-CV-05531-EJD, 2017 WL 264390 (N.D. Cal. Jan. 20, 2017) and *Shepherd v. Cancer & Hematology Centers of W. Michigan, P.C.*, No. 1:22-CV-734, 2023 WL 4056342 (W.D. Mich. Feb. 28, 2023), once presented with a factual challenge, the plaintiffs there did not present any evidence to rebut the defendant's declaration that the compromised data was not in their system. Furthermore, in *Masterson v. IMA Fin. Grp., Inc.*, No. 223CV02223HLTADM, 2023 WL 8647157, at *6 (D. Kan. Dec. 14, 2023), plaintiffs provided no expert evidence to support their claims—only a plaintiff declaration—did not plausibly explain how the compromised data could

[3] *See also Thomas Matthews v. Senior Life Insurance Company*, No. 1:24-CV-1550-MSN-LRV, 2025 WL 1181789, at *3 (E.D. Va. Apr. 22, 2025) (rejecting 12(b)(1) factual challenge to traceability and redressability of Article III standing because the facts are intertwined with the merits of Plaintiff's claim); *Dettmering v. VBit Techs. Corp.*, No. 22-cv-1482, 2023 WL 4824955, at *3 (D. Del. July 27, 2023), *report and recommendation adopted*, 2023 WL 6211243 (D. Del. Sept. 25, 2023) (denying 12(b)(1) motion that argued plaintiff's damages were not concrete); *Jackson v. Direct Bldg. Supplies LLC*, No. 4:23-cv-01569, 2024 WL 1721144, at *3 (M.D. Pa. Apr. 22, 2024) (denying a 12(b)(1) motion because motion "raises facts that go to the core of the merits").

lead to the alleged fraud and identity theft, and did not contradict the facts of defendant's declaration.

The circumstances here are different. First, even considering Comcast's inadmissible declarations, as explained more fully below, Comcast's assertion about the scope of data in ESD is unreliable. Comcast provides zero evidence as to how it created the "forensic copy" or why it created this copy nearly one month after the data breach. Nor does Comcast explain how the ESD—which is "constantly changing"—might have changed in that one-month interim before it created the copy. This raises a reliability issue that was not addressed in Comcast's cited cases. Second, Plaintiffs support this opposition with evidence, including expert declarations, that explains how access to Plaintiffs' compromised data can lead to imminent and substantial fraud and identity theft. This type of contested evidence was not presented in Comcast's cases. Third, Comcast provides zero evidence to contradict Plaintiffs' allegations that it collected the full scope of Plaintiffs' PII, such as contact information, login credentials, and Social Security numbers, in the first instance—all of which is highly sensitive PII. And fourth, nowhere does Comcast reconcile these out-of-circuit rulings with Third Circuit precedent. In fact, Comcast references the seminal case in the Third Circuit—*Davis v. Wells Fargo*, 824 F.3d 333 (3d Cir. 2016)—just one time without any analysis as to how this binding Third Circuit precedent would prevent rulings like that in *Cantinieri*, *Foster*, *Shepherd*, and *Masteron*.

Comcast has pushed past the boundary of a Rule 12(b)(1) factual attack on jurisdiction and has wandered deep into the merits of Plaintiffs' claims. If Comcast wants to challenge the merits of Plaintiffs claims before it has even answered, it should have renewed its Rule 12(b)(6) motion, which "is the proper vehicle for the early testing of [Plaintiffs'] claims." *Davis*, 824 F.3d at 349.

## III. COMCAST'S INADMISSIBLE EVIDENCE DOES NOT CONTRADICT PLAINTIFFS' DECLARATIONS AND WELL-PLED ALLEGATIONS AND SHOULD BE DISREGARDED.

On a Rule 12(b)(1) factual attack, the Court may weigh competing evidence. *Davis*, 824 F.3d at 346. But as a threshold matter, that evidence must first be admissible. *See Shelton v. Univ. of Med. & Dentistry of New Jersey*, 223 F.3d 220, 226 n.7 (3d Cir. 2000) (noting that inadmissible evidence may be considered only "if [it] is capable of admission at trial."); *Schuchardt*, 802 F. App'x at 74-76. To support its motion, Comcast generally relies on declarations of Sandra Cavazos and Adam Darrah and on attorney argument about the sensitivity of its hashed passwords. While it is unclear through which Federal Rule of Evidence Comcast is proffering its evidence (*i.e.*, FRE 602, 701, or 702), none are within reach. Thus, the Court should disregard this "evidence" when deciding Comcast's motion to dismiss.

### A. The Cavazos and Darrah declarations lack personal knowledge and are based on hearsay violating FRE 602.

The Cavazos and Darrah declarations are inadmissible because they are not based on personal knowledge but rather documents and information obtained from others. Under the Federal Rules of Evidence, a witness may testify to a matter "only if evidence is introduced sufficient to support a finding that the witness has personal knowledge of the matter." Fed. R. Evid. 602; *see Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579, 590 n.9 (1993) (quoting Advisory Committee's Notes on Fed. R. Evid. 602 ("'[T]he rule requiring that a witness who testifies to a fact which can be perceived by the senses must have had an opportunity to observe, and must have actually observed the fact'[.]" (citation omitted))). As confirmed in their depositions, Cavazos and Darrah did not observe anything asserted in their declarations. They did not observe or personally conduct any of the investigations described in their declarations nor did they independently verify the results of their investigations.

For example, in her declaration, Cavazos states that Comcast made a "forensic copy" of the contents of a data platform implicated in the 2023 data breach addressed in this litigation, the ESD. *See* ECF No. 158-3, Cavazos Decl. at ¶¶ 4-6. Cavazos states that Comcast loaded this forensic copy into a database tool called "Snowflake," and applied a series of queries against the data, resulting in the twelve Exhibits attached to the Cavazos Decl., which purportedly contain account information from the ESD concerning Plaintiffs. *Id.* at ¶¶ 11, 13. [redacted]

[redacted], and thus, are entirely inadmissible. *See Argo v. Blue Cross & Blue Shield of Kansas, Inc.*, 452 F.3d 1193, 1200 (10th Cir. 2006) (stating that "affidavits shall be made on personal knowledge," and "an affidavit is inadmissible if "'the witness could not have actually perceived or observed that which he testifies to.'"); *Lippay v. Christos*, 996 F.2d 1490, 1501 (3d Cir.1993) (vacating district court order with instructions to reconsider motion without the inadmissible hearsay evidence); *Schuchardt*, 802 F. App'x at 75 (affirming district court's ruling barring evidence on Rule 12(b)(1) factual challenge when the evidence was predicated on hearsay).

Like the Cavazos Declaration, the Darrah Declaration must also be excluded because Darrah did not have personal knowledge of the statements within, rendering it inadmissible under Fed. R. Evid. 602. Darrah asserts that ZeroFox conducted an "investigation" by searching two dark web marketplaces for data available for sale related to "Xfinity." *See* ECF No. 158-18, Darrah Decl. ¶¶ 10-11. [redacted]

[redacted], his statements must be excluded as lacking a basis in personal knowledge. *See Argo*, 452 F.3d at 1200; *Lippay*, 996 F.2d at 1501; *Schuchardt*, 802 F. App'x at 75.

In sum, neither Cavazos nor Darrah "had an opportunity to observe" or "actually observed" the matters asserted in their declarations. *Daubert*, 509 U.S. at 590 n.9. Accordingly, they lack personal knowledge as to those matters and are inadmissible under FRE 602.

**B. The Cavazos and Darrah declarations are impermissible opinion testimony violating FRE 701.**

The Cavazos and Darrah declarations should be disregarded because they contain unsupported and inadmissible opinion testimony. Federal Rule of Evidence 701 governs lay witness opinion testimony. Under FRE 701, a non-expert may provide opinions if those opinions are (a) rationally based on the perception of the witness, (b) helpful to a clear understanding of the witness' testimony or the determination of a fact in issue, and (c) not based on scientific, technical, or other specialized knowledge within the scope of Rule 702. *Acosta v. Cent. Laundry, Inc.*, 273 F. Supp. 3d 553, 555–56 (E.D. Pa. 2017). Like with FRE 602, Comcast fails to meet FRE 701.

Preliminarily, as explained earlier, Cavazos and Darrah lack personal knowledge as to the contents of their declarations, so any opinion based on that lack of personal knowledge cannot be "rationally based" as required by FRE 701(a).

Nor are Cavazos's and Darrah's declarations helpful to the determination of a fact or issue. Indeed, "...to be 'helpful,' an opinion must be reasonably reliable[.]" *United States v. Savage,* 970

F.3d 217, 286 (3d Cir. 2020). But the matters asserted in Cavazos's and Darrah's declarations are unreliable. Comcast relies on Cavazos's declaration in an attempt to limit the scope of Plaintiffs' compromised data as a result of the Data Breach. This attempt is based on Cavazos's unfounded and unexplained assertion that Comcast made a "forensic copy" of the contents of ESD implicated in the Data Breach. *See* ECF No. 158-3, Cavazos Decl. at ¶¶ 4-6. Cavazos states that Comcast imported this forensic copy into a database tool called "Snowflake," and applied a series of queries against the data, which purportedly resulted in the scope of Plaintiffs' data contained in ESD at the time of the Breach. *Id.* at ¶¶ 11, 13. Thus, the reliability of the copy created nearly a month after the Data Breach is critical to Defendants' entire defense. But Cavazos does not explain Comcast's methodology for creating the forensic copy or why it created the forensic copy almost a month after the Data Breach. A "forensic copy" is an industry standard term, and when such a copy is created improperly, it can lead to an unreliable final result. Ex. A, Strebe Decl. at ¶¶ 8-10. A couple examples include failure to export from all relevant tables or accidental use of an overly broad filter expression. *Id.* at ¶ 10. As Strebe opines, without more, the reliability of the "forensic copy" is in serious doubt. *Id.* at ¶¶ 10-16, 21.

[redacted]

[redacted] Thus, Cavazos's conclusory statement about the "forensic copy" and any evidence derived therefrom is unreliable and unhelpful. As such, Cavazos does not meet FRE 701(b). And, in any event, accepting Cavazos declaration would be inequitable and prejudicial.

Cavazos is not alone. Darrah's opinions suffer from similar deficiencies. Comcast relies on Darrah's declaration to argue Plaintiffs' information is not on the dark web site identified in the FACC. ECF No. 158-2, at 3. But to be reliable, "Rule 701 [] requires that a lay opinion witness have a reasonable basis grounded either in *experience or specialized knowledge* for arriving at the opinion that he or she expresses." *Savage*, 970 F.3d at 286 (emphasis in original). Darrah and Comcast have not shown either. [redacted]. Like Cavazos, Darrah does not meet

FRE 701(b).

Lastly, Cavazos's and Darrah's declaration contain matters that are more appropriately addressed by FRE 702. For instance, creating a forensic copy requires certain expertise to ensure that the forensic copy meets industry standard. *See* Ex. A, Strebe Decl. at ¶ 12. [redacted] Certainly, determining what is a "reasonable method" to employ to extract targeted data from a large dataset is precisely the type of opinion that requires "scientific, technical, or other specialized knowledge" for it to be reliable and meet FRE 702(c). Similarly, Darrah's declaration contains assertions about the dark web and a dark web investigation. These are unquestionably matters requiring "scientific, technical, and specialized knowledge" more appropriate under FRE 702.

**C. Comcast fails to qualify Cavazos and Darrah as expert witnesses rendering their opinions inadmissible under FRE 702.**

Likewise, because the matters asserted by Cavazos and Darrah require "scientific, technical, and specialized knowledge" within the scope of Rule 702, they must be properly qualified as expert witnesses. *See* Fed. R. Evid. 702; *Waldorf v. Shuta*, 142 F.3d 601, 625 (3d Cir. 1998). They are not. Federal Rule of Evidence 702 requires that admissible expert testimony should be considered based on qualifications, reliability, and fitness. *Id.* Preliminarily, Comcast must show that Cavazos and Darrah are qualified by "knowledge, skill, experience, training, or education[.]" Fed. R. Evid. 702. And Comcast must show that "it is more likely than not" that Cavazos's and Darrah's "scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue"; that their testimony is "based on

sufficient facts or data"; that their testimony is "the product of reliable principle and methods"; and that Cavazos's and Darrah's opinions reflect "a reliable application of the principle and methods to the facts of the case." *Id.* Comcast has not met its burden.

[redacted]

[redacted] As a result of failing to meet the first prong, the rest fall as well. Without the requisite knowledge, skill, experience, training, or education, Comcast cannot show that Cavazos's testimony is based on sufficient facts or data, is the product of reliable principles and methods, and reflects a reliable application of the principles and methods to the facts of the case.

The same issues arise with Darrah. He is not qualified by knowledge, skill, experience, training, or education. [redacted]

[redacted] Like Cavazos, without the relevant expertise or knowledge, he cannot meet the remaining requirements of FRE 702.

Cavazos and Darrah do not identify or describe any field of scientific, technical, or other specialized knowledge in which either is an expert. There is no basis from which this Court could determine that their opinions are based upon reliable principles and methods. There is no indication that Cavazos or Darrah have any appropriate basis to provide opinion testimony concerning the matters in their declarations. Their declarations should be disregarded.

**D. Comcast's attorney argument about the sensitivity of the over 30 million exposed hashed passwords does not constitute competent evidence to contradict Plaintiffs' allegations that their PII is sensitive.**

Comcast's legal argument that hashed passwords are not sensitive is not evidence and should be ignored. The Third Circuit has held that "[l]egal memorada and oral argument are not evidence and cannot by themselves create a factual dispute..." *Versarge v. Twp. of Clinton N.J.*, 984 F.2d 1359, 1370 (3d Cir. 1993) (quoting *Jersey Cen. Power & Light Co. v. Twp. of Lacey*, 772 F.2d 1103, 1109–10 (3d Cir. 1985)). Instead, "[Comcast] must resort to affidavits, depositions, admissions, and/or interrogatories" to contradict Plaintiffs' allegations. *Guidotti v. Legal Helpers Debt Resolution, L.L.C.*, 716 F.3d 764, 773 (3d Cir. 2013). Comcast provides no evidence to support its legal argument that the *crackable* hashed passwords are not sensitive. In fact, it is the opposite. From limited testing, Strebe was able to crack the hashed passwords, revealing them in plain text, with a normal computer using tools commonly used by bad actors. *See* Ex. A, Strebe Decl. at ¶¶ 19-20, 23. Plaintiffs and Class members reuse passwords across different accounts and

thus armed with these cracked passwords, bad actors can conduct account takeovers. *See* Ex. C, O'Neill Decl. at ¶¶ 11-13, 23. These cracked passwords are sensitive, and Comcast's legal argument otherwise should be disregarded.

***

Ultimately, Comcast's tactic is clear. In an effort to obtain summary judgment-like relief at the pleadings stage, Comcast tries to get away with doing much less. Comcast simply relies on scant, two-page declarations teeming with hearsay from unqualified people who lack personal knowledge about the matters asserted within and unsupported attorney argument. But no matter the procedural path, the protections built into the Federal Rules of Evidence and the Federal Rules of Civil Procedure remain. And the admissibility requirements derail Comcast's plan. If the Court does not strike Cavazos's and Darrah's declaration, then the Court should exclude them along with Comcast's unsupported legal argument about the crackable passwords when deciding the motion to dismiss.[4]

## IV. PLAINTIFFS HAVE ARTICLE III STANDING TO BRING THEIR CLAIMS IN FEDERAL COURT.

Under Third Circuit law, "Article III standing requires a plaintiff to demonstrate: (1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the

[4] Without the inadmissible declarations, Comcast's offers no competing evidence to contradict Plaintiffs' allegations. And with no contradiction of Plaintiffs' allegations, there is no factual dispute. As such, Comcast's factual attack on standing turns into a facial one. *See* C*onst. Party of Pennsylvania*, 757 F.3d at 358-59. Under a Rule 12(b)(1) facial attack, where the Court must take the allegations of the complaint as true and construe all facts in the light most favorable to Plaintiffs, Plaintiffs' allegations are more than enough to confer Article III standing. *See* Doc. 99. Indeed, Defendants confirmed as much when they removed the state court actions to federal court, asserting that the federal courts have subject matter jurisdiction. *See Fidelity & Deposit Co. of Md.*, 653 F.2d at 777 (deciding that statements made by a party "in connection with other litigation that is adverse to, or inconsistent with, its position in this case . . . is admissible as evidence against" that party).

requested judicial relief." *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 152 (3d Cir. 2022) (*Clemens II*) (quotation marks omitted); *see also TransUnion LLC v. Ramirez*, 594 U.S. 413, 432-33 (2021) (concluding that the class members whose information was "disseminated to third parties" had Article III standing). *Clemens II* and *TransUnion* foreclose any genuine dispute here.

**A. Plaintiffs plausibly establish injury-in-fact.**

To satisfy the injury-in-fact prong, Plaintiffs must allege an "actual or imminent" injury that is concrete. *Clemens II*, 48 F.4th at 152. This is not a high hurdle. As the Third Circuit emphasizes, "in the context of a *motion to dismiss* . . . the injury-in-fact element is not Mount Everest. The contours of the injury-in-fact requirement . . . are very generous, requiring only that claimant allege some specific, identifiable trifle of injury." *Blunt v. Lower Merion Sch. Dist.,* 767 F.3d 247, 278 (3d Cir. 2014) (cleaned up); *see also In re Horizon Healthcare Servs. Inc. Data Breach Litig.,* 846 F.3d 625, 633–34 (3d Cir. 2017) (same). Indeed, "at the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim." *In re Horizon,* 846 F.3d at 633–34 (quoting *Lujan,* 504 U.S. at 561) (cleaned up).

Concreteness focuses on whether the alleged harm is real and not abstract. *TransUnion*, 594 U.S. at 424. But this harm can also be intangible. *Id.* at 425. Indeed, the Supreme Court of the United States, in *TransUnion*, recognized intangible harms such as reputational harm, disclosure of private information, and intrusion upon seclusion, as being concrete. *Id.* The Court then concluded that a subset of Plaintiffs whose information was disclosed to third parties suffered a concrete harm that qualifies as an injury in fact to confer standing. *Id.* 321-433.

Critically, an injury need only be actual *or* imminent to satisfy Article III standing—it need not be both. As *Clemens II* observed, "a plaintiff need not wait until he or she has *actually* sustained

the feared harm in order to seek judicial redress, but can file suit when the risk of harm becomes imminent." *Clemens II*, 48 F.4th at 152 (emphasis in original). "This is especially important in the data breach context, where the disclosure of the data *may cause future harm* as opposed to currently felt harm." *Id.* (emphasis added). Even though "the type of data involved in a data breach may be such that mere access and publication do not cause inherent harm," a breach "can still poise the victim to endure the kind of future harm that qualifies as 'imminent.'" *Id.* Accordingly, "allegations of future injury suffice if the threatened injury is 'certainly impending' or there is a 'substantial risk' that the harm will occur." *Id.* (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014)). In other words, all that is required is a "realistic danger of sustaining a direct injury." *Id.* at 152-153 (cleaned up).

Each Plaintiff plausibly alleges actual or imminent injury-in-fact. In fact, Defendants *concede*—as they must—that eight of the thirteen Plaintiffs sufficiently allege actual, concrete injuries sufficient to satisfy the injury-in-fact requirement (though mistakenly claim that these injuries could not be traced to the Data Breach, which Plaintiffs address *infra*). For the remaining five Plaintiffs—which Defendants disingenuously describe as the "Mere Receipt Plaintiffs"—Defendants claim that none of these Plaintiffs pleads any injury-in-fact. As both a factual and a legal matter, Defendants are wrong.

Defendants mischaracterize these Plaintiffs—whose data was exfiltrated by hackers in the Data Breach but have not yet experienced confirmed misuse—as having simply "received" a Breach notice. In truth, each of these Plaintiffs alleges that their personal data—including usernames, crackable hashed passwords, partial Social Security numbers, secret questions, and other identifying information—was accessed and stolen. That data is sensitive, capable of misuse, and, under the *Clemens II* framework, its unauthorized access alone supports standing. As

Plaintiffs' expert, Mr. O'Neill, explains, these Plaintiffs are "***more than likely*** to face near-term and long-term risks of fraudulent activity." Ex. C, O'Neill Decl. at ¶ 26. Specifically:

> It is highly likely that the theft of the PII here will create a ripple effect of harm that **extends far beyond currently felt harms**, requiring both individual and systemic responses to mitigate future fraud attempts targeting the individuals whose PII was compromised by bad actors via Comcast's maintenance of PII.

*Id.* (emphasis added).

1. All Plaintiffs Face a Substantial and Imminent Risk of Identity Theft and Fraud.

The Third Circuit instructs courts to consider three non-exhaustive factors in determining whether a plaintiff has sufficiently alleged a "substantial risk" of harm: (1) whether the breach was intentional; (2) whether the data was misused—although "misuse is not necessarily required"; and (3) whether the nature of the information accessed through the data breach could subject a plaintiff to a risk of identity theft. *Clemens II*, 48 F.4th at 153-154. All these factors weigh in favor of a finding that Plaintiffs in this case face a substantial risk of harm as a result of Defendants' failure to prevent the Data Breach.

*a. The Data Breach was intentional.*

The first *Clemens II* factor—whether the Breach was intentional—strongly weighs in favor of an imminent risk of harm such that these Plaintiffs have standing. The Data Breach was not an accident or an inadvertent disclosure. It was the result of a deliberate cyberattack by malicious actors who exploited a vulnerability in Citrix's NetScaler products to gain unauthorized access to Comcast's internal systems. FACC ¶ 287.

These attackers used a critical zero-day exploit—known as the "Citrix Bleed" vulnerability—between October 16 and 19, 2023, to access and exfiltrate sensitive data belonging to approximately 36 million customers. *Id.* at 5. The exploitation of Citrix Bleed that resulted in the Data Breach was sophisticated, intentional, and targeted. *Id.* at 287. Specifically:

> After cybercriminals discovered the Citrix Bleed vulnerability, cybercriminal gangs rapidly developed custom scripts in numerous simple programming languages that could exploit NetScaler gateway devices to extract session cookies. Threat actors, particularly Lockbit 3.0 affiliates, used these scripts to automatically search for, find, and exploit NetScaler devices across the Internet, first targeting high-value network infrastructure providers such as Comcast from which they could extract valuable consumer PII. ***Use of these scripts to hack Comcast's NetScaler products demonstrates that the cybercriminals behind the Data Breach intentionally sought out Comcast's networks to extract customers' PII.***

*Id.* at 287 (emphasis added).

Moreover, Comcast received a real-time alert from its cyber incident detection system, CrowdStrike, warning of suspicious activity consistent with credential harvesting but prematurely closed the investigation after classifying it as a false positive. *Id.* at 290-294. That alert identified that a user on a NetScaler server had "engaged in suspicious activity indicative of Active Directory reconnaissance" and "[a]dversaries may attempt to find domain-level groups and permission settings." *Id.* at 290. Over the next day, a session cookie linked to that same user "queried *several hundred-thousand* additional files," plainly evidencing malicious intent. *See id.* at 293.

As a result, Plaintiffs' PII from the Breach is already circulating for sale on the dark web. *See* Ex. B, Nelson Decl. ¶¶ 8-13. In fact, "multiple sets of Comcast/Xfinity data were uploaded to a Torrent site called 'Fox Store' where cybercriminals sell and purchase stolen PII." FACC ¶ 360; Ex. B, Nelson Decl. ¶¶ 8-9, 12-13. Tellingly, it was uploaded between October 16 and 23, 2023—the first day and one week after the Data Breach. *Id.* Additional Comcast/Xfinity data affiliated with Plaintiffs and Class Members was subsequently "uploaded to BlackBet in July and September 2024." FACC ¶ 360; Ex. B, Nelson Decl. ¶ 10.

Where, as here, the Data Breach was caused by malicious actors—as opposed to an internal mistake—it is more likely to create a substantial risk of harm. *Clemens II*, 48 F.4th at 153; *see also Zimmerman et al. v. Highmark Inc.,* No. 2:23-CV-250-NR, 2025 WL 1220364, at *4 (W.D. Pa. Apr. 28, 2025) (citing *Clemens II* and ruling the intentionality of the attack supports standing

despite the hacker being unknown); *McMorris v. Carlos Lopez & Assocs.*, 995 F.3d 295, 301-03 (2d Cir. 2021) (holding that the intentional nature of an attack marshals in favor of finding standing); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 632 (7th Cir. 2007) (holding that plaintiffs had standing where a breach was "sophisticated, intentional and malicious"). Plaintiffs' allegations leave no doubt that the Breach was an intentional and targeted attack by sophisticated cybercriminals designed to harvest and sell Plaintiffs' sensitive personal data. That weighs strongly in support of finding standing.

*b. The data was misused.*

The second *Clemens II* factor—whether the data was misused—also weighs in favor of standing. Although misuse is not required to establish injury-in-fact, *Clemens II*, 48 F.4th at 154, the FACC alleges it here in spades. As an initial matter, Plaintiffs' data was misused the moment their PII was disclosed in a manner inconsistent with how Comcast represented Plaintiffs' PII would be used. In its privacy policy, Comcast promises that it will only use Plaintiffs' PII in certain circumstances and that it will only share Plaintiffs' data in limited ways, including "[a]ccount owners and other authorized users." FACC ¶¶ 354, 451. None of these circumstances involve sharing Plaintiffs' PII with unauthorized third parties. Thus, Plaintiffs' PII was misused the instance it was acquired by cybercriminals who were not authorized to receive it.

Plaintiffs also identify other instances of confirmed misuse of their PII, including fraudulent bank transfers, unauthorized purchases, phishing and social engineering attempts, and identity theft. *See* Ex. C, O'Neill Decl. ¶ 7; FACC ¶¶ 18, 30, 43, 57-59, 71, 95, 118, 133; *see generally* Ex. G, Andros Decl. ¶ 11; Ex. H, Birnie Decl. ¶ 9; Ex. I, Durham Decl. ¶ 11; Ex. J, Estevez Decl. ¶¶ 12-14; Ex. K, Fail Decl. ¶ 11; Ex. M, Nanez Decl. ¶ 10; Ex. O, Prescott Decl. ¶ 11; Ex. P, Smith Decl. ¶¶ 7-8.

Plaintiff Estevez, for example, had his Xfinity-serviced phone number stolen immediately after receiving a suspicious call from someone purporting to be from Xfinity. FACC ¶ 57; Ex. J, Estevez Decl. ¶ 12 That theft was then used to bypass two-factor authentication and initiate fraudulent wire transfers totaling $9,000 from his bank accounts, followed by an $18,000 fraud attempt on his Bank of America credit card. *Id.* at ¶¶ 57-59; Ex. J, Estevez Decl. ¶¶ 13-14; Ex. C, O'Neill Decl. ¶ 7. Similarly, Plaintiff Durham had cashier's checks fraudulently drawn from her U.S. Bank account, and a nefarious actor changed the listed address on her accounts by impersonating her in a phone call. FACC ¶ 43; Ex. I, Durham Decl. ¶ 11; Ex. C, O'Neill Decl. ¶ 7. She was actively on the phone with the bank's fraud department when a criminal attempted to move money from her account in real time. Ex. I, Durham Decl. ¶ 11. Other Plaintiffs reported unauthorized purchases, fraudulent credit card applications, and increased phishing attacks and spam tied to their compromised PII, which included partial Social Security numbers, secret questions, and crackable hashed passwords—data often used as a first line of authentication for account access, including by Comcast itself. FACC ¶¶ 18, 30, 71, 95, 118, 133; Ex. G, Andros Decl. ¶ 11; Ex. H, Birnie Decl. ¶ 9; Ex. K, Fail Decl. ¶ 11; Ex. M, Nanez Decl. ¶ 10; Ex. O, Prescott Decl. ¶ 11; Ex. P, Smith Decl. ¶ 11; Ex. C, O'Neill Decl. at ¶¶ 7-23.

This pattern of activity is consistent with cybercriminals actively misusing stolen data. *See* Ex. B, Nelson Decl. ¶¶ 12-13; Ex. C, O'Neill Decl. ¶ 27. As the O'Neill declaration emphasizes, Plaintiffs are at substantial risk for further fraud given the combination of identifiers stolen *and the demonstrated presence of this data on dark web markets*—including uploads to "Fox Store" and "BlackBet," where Comcast/Xfinity customer data was offered for sale. FACC ¶ 360; Ex. B, Nelson Decl. ¶¶ 12-13; Ex. C, O'Neill Decl. ¶ 26. This is a classic example of real-world misuse by sophisticated criminal actors.

Faced with this evidence of misuse, Defendants ask the Court to ignore it for a subset of five Plaintiffs—arguing that because these Plaintiffs did not already experience such injuries, they cannot "bootstrap" standing. But this puts the cart before the horse. The presence of actual misuse caused by the Breach demonstrates that the risk of harm is substantial—even for Plaintiffs who have not yet experienced fraud or identity theft. Plaintiffs asserting standing based on imminent risk need not demonstrate past harm themselves. As *Clemens II* instructs, "a plaintiff need not wait until he or she has actually sustained the feared harm in order to seek judicial redress, but can file suit when the risk of harm becomes imminent." *Clemens II*, 48 F.4th at 152.

Where, as here, Plaintiffs allege "that at least some part of the compromised dataset has been misused—even if plaintiffs' *particular* data subject to the same disclosure incident has not yet been affected . . . courts have been more likely to conclude that plaintiffs have established a substantial risk of future injury." *McMorris*, LLC, 995 F.3d at 301 (emphasis in original); *see also Clemens II*, 48 F.4th at 154-55 n.4 (observing that "any misuse of the data, even if the class representative has not yet been affected, cuts towards standing.").[5] Plaintiffs' evidence of actual misuse of PII obtained in the Breach as to some Plaintiffs supports—rather than undermines—the

[5] *See also In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1263 (11th Cir. 2021) (finding that some allegations of actual misuse or actual access to personal data support Article III standing for a data breach based on an increased risk of theft or misuse); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 n.7 (9th Cir. 2018) (explaining that although the specific plaintiffs had not experienced any fraudulent activity, allegations that other customers whose data was compromised in the same data breach had reported fraudulent activity helped establish that the plaintiffs were at a substantial risk of fraud); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) (concluding it is plausible to infer a substantial risk of harm from data breach where only a subset of plaintiffs have experienced fraudulent activity); *see also In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 58 (D.C. Cir. 2019) ("[A] hacker's 'intent' to use breach victims' personal data for identity theft become markedly less important where, as here, several victims allege that they have *already* suffered identity theft and fraud as a result of the breaches.") (emphasis in original); *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 375 (1st Cir. 2023) ("That at least some information stolen in a data breach has already been misused also makes it likely that other portions of the stolen data will be similarly misused.").

inference that *all* Plaintiffs face a substantial and imminent risk of harm.[6]

In short, the presence of actual misuse eliminates any question of whether Plaintiffs face a substantial risk of future harm—many already have. This factor cuts toward standing for all Plaintiffs.

*c. The nature of the data puts Plaintiffs at risk of identity theft.*

The third *Clemens II* factor—whether the information exposed can enable identity theft and fraud—squarely supports a finding of injury-in-fact. Comcast's breach involved precisely the types of data that courts recognize create a substantial risk of harm, including personal information (names, addresses, phone numbers, and dates of birth), password information (user IDs, crackable hashed passwords, and secret questions and answers), and account information (account numbers and partial Social Security numbers). Ex. C, O'Neill Decl. ¶ 8; FACC ¶ 3.

Standing alone, these data points are sensitive. *See Clemens II,* 48 F.4th at 154 ("For instance, disclosure of social security numbers, birth dates, and names is more likely to create a risk of identity theft or fraud."); *see also* Ex. C, O'Neill Decl. at ¶ 10. But when a combination of this data is stolen—as occurred here—they create a blueprint for identity theft, compromised accounts, and fraud. Ex. C, O'Neill Decl. ¶ 10 ("[W]hen these data points are exposed in combination with one another, as in this data breach, they significantly increase the likelihood of identity theft and fraud."); FACC ¶¶ 247, 361, 364. Comcast's own Notice acknowledged that the breached information could be used to access customer accounts and any information stored therein, and urged Plaintiffs to take immediate steps to protect themselves. FACC ¶¶ 87, 109, 147, 159, 170.

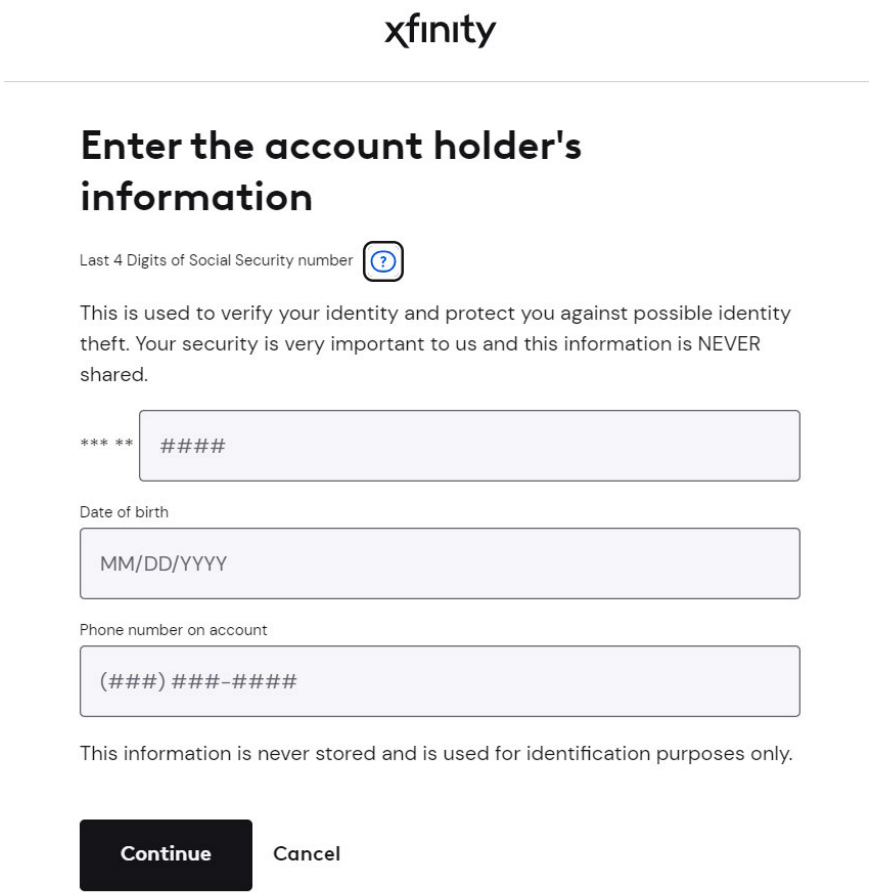
[6] Curiously, the dataset that Darrah purchased from the dark web includes the similar information as to that data Comcast identified in the notice letters to its customers. *See* 158-18, at Ex. D02. This further supports the link between this information posted to Black Bet and the Data Breach.

Defendants now claim that only a "subset" of this information was accessed for certain Plaintiffs and argue that absent full SSNs or financial account numbers, the data stolen in the breach is not sensitive enough to support standing. That argument fails for two reasons. First, as explained above, this Court should not credit Defendants' unreliable, after-the-fact assertions that Plaintiffs' breached data did not involve the information Comcast identified in its own notices to Plaintiffs. *See supra*, Part III. Second, even if the attackers only exfiltrated a subset of the data previously identified for each Plaintiff, the data indicated in Comcast's declaration materials was still highly sensitive and subjects Plaintiffs to a substantial risk of identity theft and fraud.

(1) Comcast's notice identified highly sensitive data.

Comcast's own notice to Plaintiffs confirms that the compromised data was highly sensitive. According to Comcast, compromised PII included names, contact information, dates of birth, partial Social Security numbers, usernames and hashed passwords, and secret questions and answers. FACC ¶ 317. This is precisely the kind of information that can be used to commit fraud and identity theft.

Indeed, armed only with the last four digits of a Social Security number, a date of birth, and a phone number, cybercriminals can bypass identity verification protocols used by banks, cell providers, and even Comcast itself. In fact, the data compromised in the Breach is *the same information* Comcast uses to verify its own customers' identities:




In short, the Data Breach subjects Plaintiffs to a single point of compromise. As a result of the breach, "hackers can access the victim's internal Comcast account," which in turn provides access to "stored personal data, including payment card information and billing/purchase history." Ex. C, O'Neill Decl. ¶ 23. This makes Plaintiffs vulnerable to actual account takeovers, unauthorized purchases, and credential-based fraud, rather than some abstract, speculative threat. *Id.* Their PII is not lying dormant. It is actively circulating for sale on the dark web—and readily weaponizable by cybercriminals. FACC ¶ 360; Ex. B, Nelson Decl. ¶¶ 8-13; Ex. C, O'Neill Decl. ¶¶ 23-27.

In their motion, Defendants argue for the first time that the attackers only exfiltrated a

"subset" of some Plaintiffs' PII. ECF No. 158-2, at 23. As explained earlier, that argument relies on unreliable, after-the-fact evidence offered solely to support their motion. *See supra*, Part III. This Court should not afford it any weight.

But even accepting Defendants' litigation-driven assertions about what data was compromised, the exposed information remains highly sensitive and can be used by cybercriminals to perpetrate a range of fraud and identity theft. As the explained in the following paragraphs, the combination of compromised data for each Plaintiff (according to Comcast's declarations) falls into three distinct, high-risk categories—any of which are independently capable of enabling identity theft, account takeover, or financial fraud. Ex. C, O'Neill Decl. ¶¶ 8-9.

***Partial SSN Plaintiffs.*** According to Comcast, the cyberattacker exfiltrated the last four digits of the Social Security numbers for Plaintiffs Estevez, Hendrickson, Nunn, and Wilson, along with other identifying information. *Id.* ¶ 8.[7] Defendants downplay the significance of this data—but courts routinely recognize that partial SSNs, when combined with other PII, can be used to pass identity verification protocols and reconstruct full SSNs. *See*, *e.g.*, *Myers v. Equifax Info. Servs., LLC*, No. 120CV00392JMSDLP, 2021 WL 4992649, at *3 (S.D. Ind. Oct. 27, 2021) (last four digits are "frequently used to confirm identity" and "valuable to identity thieves"); *O'Brien v. Smoothstack, Inc.*, No. 1:23-CV-491, 2024 WL 1356674, at *10 (E.D. Va. Mar. 28, 2024) (prohibiting disclosure of the last four digits because they are "sensitive and personal information"); *White v. Integrated Elec. Tech., Inc.*, No. 12-359, 2013 WL 2903070, at *10 (E.D. La. June 13, 2013) (recognizing "the significant privacy and security concerns inherent in disclosing the last four digits of class members' Social Security numbers"); FACC ¶ 247.

[7] According to Comcast, these Plaintiffs' breached PII also included at least their names, phone numbers, and physical/billing address. *Id.*

At least one court has addressed the sensitivity of the last four digits of a Social Security number and resulting risks in the context of a data breach. In *Greek Islands Cuisine, Inc. v. YourPeople, Inc.*, No. 4:24-CV-5045-TOR, 2024 WL 5223144, at *2 (E.D. Wash. Dec. 26, 2024), the court found standing where the last four digits of a Social Security number was taken in a data breach. That court found the last four digits of a Social Security number combined with a full name "is sensitive information." *Id.* at *4. In doing so, rejected Defendants' same argument pointing to Federal Rule Civil Procedure 5.2, stating that "there is more than a remote possibility that a third-party may use the combination of Plaintiffs' name and partial social security numbers to gain access again to other financial accounts they already hold." *Id.* The Court also emphasized the note to Rule 5.2: "'[w]hile providing for the public filing of some information, such as the last four digits of an account number, the rule does not intend to establish a presumption that this information never could or should be protected.'" *Id.* While the court only found standing based on the fact that criminals could continue access existing bank accounts and not open a new account, that Court did not address the ability for threat actors to reverse engineer Social Security numbers as they can predict the first five numbers based on public and semi-public data. *See* Ex. C, O'Neill Decl. ¶¶ 17-19.

Consistent with prevailing case law, numerous other sources provide that the last four digits of a Social Security number "is highly sensitive information that if exposed, whether in isolation or with other pieces of data, places an individual at substantial risk of fraud and identity theft." Ex. C, O'Neill Decl. ¶ 15; FACC ¶ 244. Partial Social Security numbers are commonly used for authentication by financial institutions, healthcare providers, credit bureaus, and other companies, including Comcast. Ex. C, O'Neill Decl. ¶ 16; FACC ¶ 247. According to Aura, a leading identity theft protection and credit monitoring company, cybercriminals armed with the last four digits of

an individual's Social Security number, in combination with other personal information—as is the case here—"can open accounts, access an individual's name, or apply for benefits in that person's name." FACC ¶ 247. That is why the Federal Trade Commission "warns against sharing even partial Social Security numbers, as scammers can use them to commit identity theft." *Id.*

Moreover, when paired with a Plaintiff's name and date of birth—both of which were also compromised in the Data Breach—malicious actors can "reconstruct" a full Social Security number. O'Neill Decl. ¶ 19; FACC ¶¶ 247-48. Cybercriminals can do so because first five digits identify "when and where a person is born," and only the last four digits are randomized. *Id.* Reverse-engineering a full Social Security number is not hypothetical or speculative—it is a genuine threat. A study conducted by researchers at Carnegie Mellon University demonstrated that hackers can "accurately predict the first 5 digits of a Social Security number using public or semi-public sources." Ex. C, O'Neill Decl. ¶ 19.

Unlike most other personal information, Social Security numbers are "permanent identifiers that cannot easily be changed." FACC ¶ 251. That means that once a Social Security number is exposed, a Plaintiff is at risk of identity theft *indefinitely*. *Id.* Data breach victims thus often face multiple incidents of fraud over their lifetime due to criminals reusing stolen data. *Id.* Even a partial Social Security number becomes a ready-made key for identity theft, fraud, phishing, and SIM swap attacks—highlighting just how sensitive this information is. Ex. C, O'Neill Decl. ¶ 23.

***Password Plaintiffs.*** According to Comcast, the attacker also exfiltrated usernames, hashed passwords, and account numbers for nearly every Plaintiff. Ex. C, O'Neill Decl. ¶ 10.[8]

[8] Password Plaintiffs' exfiltrated data also included names, phone number, physical address, and email addresses. *Id.*

While Defendants suggest that hashed passwords do not present a meaningful risk, that assumption ignores how easily compromised this data can be in practice. FACC ¶ 252. The hashing algorithm Comcast used is vulnerable to common cracking methods employed by threat actors. Ex. A, Strebe Decl. at ¶¶ 17-20, 23. Indeed, Strebe was able to crack numerous "hashed" passwords stored by Plaintiffs in Comcast's system, revealing them in plain text. *Id.* Preliminarily, the ease with which cybercriminals can un-hash users' passwords means that any PII in Plaintiffs' Comcast accounts at the time of the breach, including sensitive payment and financial information, may also be in the hands of cybercriminals. Ex. A, Strebe Decl. ¶¶ 17-20; Ex. C, O'Neill Decl. at ¶ 25.

But the risks from stolen login credentials go well beyond unauthorized access to Plaintiffs' Comcast accounts. The de-hashed credentials stolen here can be used in credential stuffing attacks to access users' *other* accounts, as well. In "credential stuffing" attacks, threat actors gain access to users' other online accounts by engaging in mass "stuffing" of the stolen credentials and seeing if they grant access to accounts on other lucrative websites and applications. *See* Ex. C, O'Neill Decl. ¶¶ 12-13, 23; FACC ¶¶ 371-72 (noting this makes Plaintiffs "particularly at risk" of additional data breaches). This practice takes advantage of the fact that, in an age where most individuals have more website accounts than they can keep track of, individuals typically reuse passwords on at least ten of their personal accounts. FACC at ¶ 252; Ex. C, O'Neill Decl. ¶¶ 13, 23. Stolen passwords also provide an entry point for phishing campaigns, social engineering, and identity fraud, particularly when combined with the other stolen PII, including names and email addresses. Ex. C, O'Neill Decl. ¶ 23. Courts have recognized that access to login credentials—especially in conjunction with other identifiers—thus creates a substantial risk of harm. *See*, *e.g.*, *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *12-13 (N.D. Cal. Aug. 30, 2017) (holding compromise of user credentials supported standing).

Defendants' assertion that "hashing" alone "transforms plaintext passwords into an unintelligible series of numbers and letters" that is "computationally infeasible" to crack is demonstrably wrong. As Plaintiffs' experts prove, Comcast's weak encryption allows any hacker to quickly crack the hashing and reveal Plaintiffs' stolen passwords in plain text—enabling immediate, unauthorized access to sensitive financial data, private communications, and other accounts. *See* Ex. A, Strebe Decl. ¶¶ 17-20, 23; Ex. C, O'Neill Decl. ¶¶ 12-13, 23.

***Secret Q&A Plaintiffs.*** Comcast's notice also confirmed that customers' security questions and answers were part of the trove of compromised data. Ex. C, O'Neill Decl. ¶ 20.[9] While Defendants again downplay the sensitivity of this information, courts and experts recognize that secret questions and answers are a critical line of defense in online authentication—and create substantial risks to individuals when breached. FACC ¶ 253; *see Huynh v. Quora, Inc.*, No. 18-CV-07597-BLF, 2019 WL 11502875, at *5 (N.D. Cal. Dec. 19, 2019) (finding standing because security questions and answers, along with other identifying information, is "sufficiently similar to a social security number"); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *12-13 (holding compromise of security questions supported standing).

Like usernames and passwords, security questions and answers are "commonly repeated across various websites," and often involve sensitive information like a person's mothers' maiden name or city of birth. *Id.* The answers to these questions put Plaintiffs at risk for further breaches to their other online accounts. Ex. C, O'Neill Decl. ¶ 23 (noting "it is likely the hashed secret answers can be cracked as well"). These answers give hackers the tools to reset passwords, bypass multi-factor authentication, and impersonate victims across a wide range of services. *Id.* at ¶ 23.

[9] Security Q&A Plaintiffs exfiltrated data also included user IDs, email addresses, and hashed (but decipherable) passwords. *Id.*

Even the questions alone may reveal clues that allow a criminal access to a highly sensitive online account. *Id.* at ¶ 21.

Stolen security question and answer data also enables targeted phishing and social engineering, allowing attackers to easily deceive victims with high credibility. *Id.* at ¶ 23. And this type of information is especially dangerous when combined with other PII such as usernames, emails, and account numbers—all of which were also compromised in the Data Breach. *Id.*; *In the Matter of James V. Grago, Jr., individually and d/b/a ClixSense.com*, 2019 WL 1932140, at *4 (F.T.C. Apr. 24, 2019) (finding misuse of security questions "is likely to facilitate identity theft, privacy harms, and other consumer injuries"). The compromise of these security questions and answers leaves Plaintiffs vulnerable to immediate exploitation—supporting their standing based on a substantial risk of future harm.

(2) This highly sensitive data supports standing.

Each category of compromised data—whether passwords, partial Social Security numbers, or security questions and answers—poses a substantial risk of identity theft and fraud. That risk is not speculative or attenuated; it is real, immediate, and well-recognized by courts evaluating injury-in-fact under Article III. *See Clemens II*, 48 F.4th at 152–54.

*Clemens II* makes clear that Plaintiffs need not wait until harm occurs to establish standing. It is enough that the disclosure of their PII subjects them to a substantial risk of future misuse. *Id.* at 152. Contrary to Defendants' arguments, no Plaintiff is required to show that their specific combination of data matches some predetermined legal threshold. The Third Circuit explicitly rejected that sort of rigid checklist. *Id.* at 154 (noting that even data that does not cause "inherent harm" may still cause future harm that qualifies as "imminent").

The data at issue here meets that standard. As Plaintiffs explain at length in the FACC and

expert declarations, even subsets of the compromised PII, taken alone, can enable unauthorized access, financial exploitation, and account takeovers. Ex. C, O'Neill Decl. ¶¶ 10, 23. When those subsets are paired with other identifying information, the risks only increase. *Id.*

In addition to credential stuffing attacks and account takeovers, Plaintiffs face the imminent risk of phishing and social engineering attacks, as well as SIM swapping and port-out fraud. *Id.*[10] The risk of SIM-swap attacks and port-out fraud is particularly acute. These attacks allow a threat actor to intercept multifactor authentication codes sent to an individual's phone number—enabling access to individuals' most sensitive information, including bank accounts, medical records, and confidential cloud-based storage data. *Id.* Cybercriminals can even monitor and respond to the victim's private texts and phone calls. *Id.* This is exactly what happened to Plaintiff Estevez as a result of the Breach—resulting in two fraudulent wire transfers that drained $9,000 from his bank accounts. FACC ¶¶ 57-59; Ex. J, Estevez Decl. ¶¶ 12-14; Ex. C, O'Neill Decl. at ¶ 23.

Plaintiffs whose PII have been compromised further face the ongoing risk of identity fraud, tax fraud, medical identity theft, and long-term reputational damage. Ex. C, O'Neill Decl. ¶ 23. *Clemens II* recognizes that these kinds of risks—particularly where, as here, they are supported by particularized facts and expert opinions—are more than sufficient to establish injury-in-fact.

Defendants rely on a handful of district-court cases from other circuits and data-breach notification laws to claim the compromised data here is not sensitive.[11] They cite no case, however,

[10] A SIM-swap attack is a scheme in which a hacker commandeers a victim's mobile phone number and intercepts confidential communications intended for the victim, including text messages used to verify a victim's financial, medical, and personal accounts. FACC ¶¶ 258-260, 366. Similarly, in port-out fraud, a hacker uses PII obtained in a data breach to port a victim's mobile phone service to a different cellular provider—allowing them unfettered access to their phone service. *Id.*

[11] These cases do not stand for this proposition or are easily distinguishable. *See In re VTech Data Breach Litig.*, No. 15-CV-10889, 2017 WL 2880102 (N.D. Ill. July 5, 2017) (failing to address whether the information was "highly sensitive" or allege that Social Security numbers were

where a court found that the *combination* of the PII exposed here was anything but "sensitive." Nor could they. As explained above, each of these kinds of information enables immediate access to a treasure trove of highly sensitive accounts and information. Indeed, Comcast itself allows customers to access their account and verify their identity simply by providing the last four digits of a Social Security number, date of birth, and phone number—the very information stolen by hackers in the Data Breach. Ex. C, O'Neill Decl. ¶¶ 18, 23.

Defendants lean heavily on the claim that only the last four digits of Plaintiffs' Social Security numbers were stolen in the attack—instead of the full nine-digit numbers. But as Plaintiffs have explained, federal courts have consistently recognized that even a *partial* Social Security number is extraordinarily sensitive information that exposes its owner to a substantial risk of harm, if exposed. *See*, *e.g.*, *Greek Islands Cuisine, Inc.*, 2024 WL 5223144, at *4 (finding last four digits of SSN to be sufficiently sensitive to confer Article III standing); *Smoothstack, Inc.*, 2024 WL 1356674, at *10 (rejecting request to compel party to disclose the last four digits of individuals SSNs because that data is "sensitive and personal information"); *Myers*, 2021 WL 4992649, at *3 (rejecting argument that the federal rules strip consumers of the "privacy interest in the last four digits of his or her SSN" and concluding they are "frequently used to confirm identity in various settings and that, combined with other personal information, could be valuable to identity thieves"); *White*, 2013 WL 2903070, at *10 ("[T]he court recognizes the significant privacy and

disclosed); *Antman v. Uber Techs., Inc.*, No. 15-CV-01175, 2018 WL 2151231, at *10 (N.D. Cal. May 10, 2018) (failing to allege Social Security number or "other information that an ID thief could use" was disclosed); *Rahman v. Marriott Int'l, Inc.*, No. 20-cv-00654, 2021 WL 346421, at *2 (C.D. Cal. Jan. 12, 2021) (failing to allege Social Security number was disclosed); *Cooper v. Bonobos, Inc.*, No. 21-CV-854 (JMF), 2022 WL 170622, at *4 (S.D.N.Y. Jan. 19, 2022) (same); *Kylie S. v. Pearson PLC*, 475 F. Supp. 3d 841, 844 (N.D. Ill. 2020) (same); *Jackson v. Loews Hotels, Inc.*, No. CV18827, 2019 WL 2619656, at *5 (C.D. Cal. Jan. 4, 2019) (same); *Brett v. Brooks Bros. Grp.*, No. CV 17-4309-, 2018 WL 8806668, at *3 (C.D. Cal. Sept. 6, 2018) (same); *Yankovich v. Applus Techs., Inc.*, 621 F. Supp. 3d 269, 278 (D. Conn. 2022) (same).

security concerns inherent in disclosing the last four digits of class members' Social Security numbers."); *Humphries v. Stream Int'l, Inc.*, No. 3:03-CV-1682, 2004 U.S. Dist. LEXIS 20465, at *12 (N.D. Tex. Feb. 13, 2004) (denying request that defendants produce the last four digits of class members' SSNs because they are "highly personal information").[12]

Defendants further claim that the last four digits of a Social Security number are not "sufficiently sensitive" because several states' data breach laws allegedly do not require a notice when such data is stolen. ECF No. 158-2, at 18. But this claim is misleading. Most state statutes do not distinguish between full and partial Social Security numbers. Rather, they simply include a general reference to Social Security numbers in the list of PII that mandates sending a data-breach notice. *See*, *e.g.*, Cal. Civ. Code § 1798.82(h) (defining "personal information" to include a "Social Security number" in combination with a person's name). In fact, Rhode Island expressly recognizes the sensitivity of even partial SSNs and prevents their disclosures on the outside of postcards and envelopes. *See* R.I. Gen. Laws § 6-48-8 (protecting "all *or part* of an individual's Social Security number") (emphasis added).

Similarly, hashed passwords and secret questions and answers are highly sensitive information that allow hackers to perpetrate fraud and identity theft. *See Huynh*, 2019 WL 11502875, at *5 (finding standing because security questions and answers, along with other identifying information, is "sufficiently similar to a social security number"); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *12-13 (holding compromise of passwords and security questions supported standing). In fact, the same data-breach notification

[12] *See also Fleming v. Parnell*, No. 13-cv-5062, 2013 WL 4511494, at *5 (W.D. Wash. Aug. 23, 2013) (ordering the last four digits of employees' SSNs be produced under Attorneys' Eyes Only designation given their "highly sensitive nature"); *Byard v. Verizon W. Virginia, Inc.*, 287 F.R.D. 365, 377 (N.D.W. Va. 2012) (refusing to compel last four digits of SSNs because "employees clearly have substantial privacy concerns associated with their social security numbers").

laws that Comcast cites require notification about the PII at issue here. *See* Cal. Civ. Code § 1798.29 (defining personal information to include a person's name in combination with a username or email address in combination with a security question and answer).[13] That is because this information enables infiltration of financial accounts, medical records, and confidential communications, thereby creating an imminent and substantial risk of further harm. Ex. C, O'Neill Decl. at ¶ 23.

* * *

Even in the face of evidence that the Breach was malicious—and the release of Plaintiffs' highly sensitive data on the dark web—Defendants still contend that Plaintiffs lack standing because they are not at imminent risk of harm. That argument ignores the alarming reality that every Plaintiff now faces.

Defendants primarily rely on *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011)—a decision that predates more than a decade of developments in data-breach law and has since been clarified and substantially narrowed by the Third Circuit. In any event, it is readily distinguishable. In *Reilly*, the court found no standing where the plaintiffs could not allege that a breach had even occurred, let alone that any data had been exfiltrated or misused. *Id.* at 40–42. The court emphasized that plaintiffs relied only on *speculation* that a hacker might eventually read and misuse their data. *Id.* at 44. This case is not *Reilly*.

Here, Plaintiffs do not rely on speculation. Rather, they allege that Comcast suffered a targeted cyberattack perpetrated by sophisticated threat actors, that those actors exfiltrated

[13] *See also* 6 Del. Code Ann. § 12B-101 (same); Fla. Stat. § 501.171 (a username or email address in combination with a security question and answer); 815 Ill. Comp. Stat. § 530/5 (same); N.J. Stat. Ann. § 56:8-161 (a person's name in combination with a username or email address and a security question and answer); 73 P.S. § 2302 (same).

Plaintiffs' data, and that the stolen data—including usernames, passwords, partial Social Security numbers, and other sensitive personal information—is now circulating on the dark web. FACC ¶¶ 287, 317, 360; Ex. B, Nelson Decl. ¶¶ 8-13. Unlike in *Reilly*, several Plaintiffs have already experienced fraud and identity theft; others now face an imminent risk of suffering the same harms. *Id.* at ¶¶ 18, 30, 43, 57-59, 71, 95, 118, 133; *see also* Ex. G, Andros Decl. ¶ 11; Ex. H, Birnie Decl. ¶ 9; Ex. I, Durham Decl. ¶ 11; Ex. J, Estevez Decl. ¶¶ 12-14; Ex. K, Fail Decl. ¶ 11; Ex. M, Nanez Decl. ¶ 10; Ex. O, Prescott Decl. ¶ 11; Ex. P, Smith Decl. ¶ 11. None of these harms are hypothetical—they are exactly the types of risks that the *Clemens II* court later found sufficient to support standing.

This case is, in nearly every material respect, a mirror image of *Clemens II*. There, the Third Circuit found standing based on allegations that a hacking group intentionally targeted the defendant, stole sensitive personal data, and posted it on the dark web—subjecting those plaintiffs to risk of identity theft and requiring them to engage in increase monitoring efforts. *Clemens II*, 48 F.4th at 157-58. The same is true here. Plaintiffs allege a targeted cyberattack by sophisticated threat actors, the exfiltration and dark web circulation of their PII, and both actual misuse and substantial risk of future harm. FACC ¶¶ 5, 287, 317, 360; Ex. B, Nelson Decl. at ¶¶ 8-13, Ex. C, O'Neill Decl. ¶ 23. As in *Clemens II*, Plaintiffs have also taken extensive steps to mitigate the fallout, including spending time and money on credit monitoring and fraud prevention efforts. FACC ¶¶ 20, 61, 73, 85, 97, 120, 134, 145, 157, 168; *see also, e.g.*, Ex. J, Estevez Decl. ¶ 17; Verdier Decl. ¶ 13, attached as Exhibit Q. Plaintiffs have therefore established injury-in-fact.

2. Plaintiffs' Injuries Are Concrete.

Initially, like in the subset of plaintiffs in *TransUnion*, Plaintiffs here suffered a concrete injury the moment their private information was disclosed to unauthorized third parties. *See*

*TransUnion*, 594 U.S. at 432-33 (concluding that the class members whose information was "disseminated to third parties" had Article III standing).

In addition, as the Third Circuit recognizes, a plaintiff has suffered concrete injury in the data breach context, "where the asserted theory of injury is a substantial risk of identity theft or fraud" and the plaintiff "alleges that the exposure to that substantial risk caused additional, currently felt concrete harms." *Clemens II*, 48 F.4th at 155-56. "For example, if the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury." *Id.* at 156. Plaintiffs easily clear that bar here.

As explained above, each Plaintiff has either (1) experienced actual injuries like fraud or identity theft or (2) faces an imminent risk of suffering the same harms. FACC ¶¶ 18, 30, 43, 57-59, 71, 95, 118, 133; *see also generally* Exhibits G–S. To satisfy concreteness, these at-risk Plaintiffs need only allege the Data Breach caused them to suffer additional harm, such as mitigation measures, lost time, or emotional distress. *See Clemens II*, 48 F.4th at 156. Plaintiffs have done exactly that. They allege that they spent time and money mitigating their risk, including canceling accounts, changing passwords, replacing debit cards, instituting credit freezes, and subscribing to credit monitoring and fraud prevention services. FACC ¶¶ 20, 61, 73, 85, 97, 120, 134, 145, 157, 168; Ex. G, Andros Decl. ¶ 13; Ex. H, Birnie Decl. ¶ 11; Ex. I, Durham Decl. ¶ 13; Ex. J, Estevez Decl. ¶ 17; Ex. K, Fail Decl. ¶ 14; Hendrickson Decl. ¶ 13, attached as Exhibit L; Ex. M, Nanez Decl. ¶ 12; Nunn Decl. ¶ 10, attached as Exhibit N; Ex. O, Prescott Decl. ¶ 13; Ex. P, Smith Decl. ¶ 13; Ex. Q, Verdier Decl. ¶ 13; Wilson Decl. ¶ 8, attached as Exhibit R; Wolfson Decl. ¶ 10, attached as Exhibit S. Each Plaintiff also alleges that they have experienced stress, fear, emotional distress, and anxiety as a direct consequence of the Breach. FACC ¶¶ 21, 34, 47, 62, 74,

86, 98, 108, 121, 135, 146, 158, 169; Ex. G, Andros Decl. ¶ 18; Ex. H, Birnie Decl. ¶ 16; Ex. I, Durham Decl. ¶ 18; Ex. J, Estevez Decl. ¶ 22; Ex. K, Fail Decl. ¶ 19; Ex. L, Hendrickson Decl. ¶ 16; Ex. M, Nanez Decl. ¶ 16; Ex. N, Nunn Decl. ¶ 14; Ex. O, Prescott Decl. ¶ 18; Ex. P, Smith Decl. ¶ 13; Ex. Q, Verdier Decl. ¶ 18; Ex. R, Wilson Decl. ¶ 13; Ex. S, Wolfson Decl. ¶ 15. These are concrete harms. S*ee In re Equifax Inc.*, 999 F.3d at 1262 (holding that "when a plaintiff faces a sufficient risk of harm, the time, money, and effort spent mitigating that risk are also concrete injuries"); *Clemens II*, 48 F.4th at 158 (holding that emotional distress injuries and money spent mitigating a breach are concrete harms); *In re Numotion Data Incident Litig.*, 3:24-CV-00545, 2025 WL 57712, at *16 (M.D. Tenn. Jan. 9, 2025) ("[T]he court finds that the plaintiffs have adequately alleged facts that, if true, would entitle them to recover the reasonable and necessary cost of future credit monitoring, given the type of data stolen and the fact that, according to the plaintiffs, the information has already been published on the dark web.").

These injuries are not abstract. The time, money, and emotional damage associated with responding to the Breach are ongoing and measurable consequences of Defendants' failure to adequately safeguard Plaintiffs' sensitive personal information. Plaintiffs therefore have suffered a concrete injury sufficient to confer Article III standing.

**B. Plaintiffs' injuries are fairly traceable to the Data Breach.**

Along with a substantial risk of identity theft and fraud, certain Plaintiffs also allege an injury based on fraudulent activity. Their alleged fraudulent activity is fairly traceable to Defendants.

Plaintiffs plausibly allege and the evidence shows instances of fraud that are fairly traceable to the Data Breach. Traceability means that "the injury was caused by the challenged action of the defendant as opposed to an independent action of a third party." *Clemens II*, 48 F.4th at 158. "Proximate causation is not a requirement of Article III standing, which requires only that the

plaintiff's injury be fairly traceable to the defendant's conduct." *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 134 n.6 (2014). Either but-for causation or concurrent causation is necessary to satisfy traceability. *Id.* And "standing may be satisfied even if the plaintiff alleges an indirect (or multistep) causal relationship between the defendant's conduct and her injury." *LaSpina v. SEIU Pennsylvania State Council*, 985 F.3d 278, 287 (3d Cir. 2021). The burden to establish causation at the pleading stage is not a heavy one. *Mielo v. Steak 'n Shake Operations, Inc.*, 897 F.3d 467, 481 (3d Cir. 2018). And Plaintiffs have met their burden at this early stage. Nonetheless, Defendants still challenge traceability. In doing so, Comcast makes a factual attack and Citrix a facial attack. Both attacks fail.

1. Comcast's factual attack on traceability fails.

Comcast argues that a subset of Plaintiffs cannot identify misuse because the information contained in ESD at the time of the Data Breach cannot be connected to their alleged fraud and identity theft. Comcast is mistaken. To start, as explained above in Part III, Comcast has not met its burden of proffering competent evidence to establish that the purported forensic copy created nearly a month after the Breach included the full extent of Plaintiffs' compromised data. Thus, Comcast's traceability argument relies on its own self-serving and inadmissible declaration. But even if the Court accepts Comcast's submissions as fact, Plaintiffs still establish traceability.

In addition through their well-pleaded allegations, Plaintiffs establish their injuries are connected with—*i.e.*, fairly traceable to—the Data Breach and the failures by Comcast that led to it. *See also Roma v. Prospect Medical Holdings, Inc.*, 2024 WL 3678984, at *7 (E.D. Pa. Aug. 6, 2024) (concluding that the allegation that the defendant "'fail[ed] to implement adequate data security measures and protocols to properly safeguard and protect' data in its custody 'from a foreseeable cyberattack . . . [t]hat led to its publication on the dark web" was sufficient to establish

a causal link). Plaintiffs allege their information was actually stolen from Comcast's systems due to Comcast's action or inaction: Comcast's data security failures. Plaintiffs allege their stolen PII is circulating on the Dark Web. And Plaintiffs allege concrete tangible harms in the form of identity theft and fraud that occurred after the Breach involving the same information stolen in the Breach. Plaintiffs also allege they are at an imminent risk of harm and have suffered damages in the form of mitigation costs and emotional distress resulting from the Data Breach.

Plaintiffs' allegations are confirmed by the evidence. In response to Comcast's efforts to introduce information outside of the pleadings, Plaintiffs provide further evidence that their injuries are fairly traceable to the Data Breach. Each named Plaintiff here submits a sworn declaration discussing the causal connection between their injuries and the Data Breach. Plaintiffs also provide expert evidence to rebut Comcast's attack on traceability. The opinions of Plaintiffs' cybercriminal investigation expert, Matthew O'Neill, offer further evidence Plaintiffs' injuries are sufficiently traceable to the Data Breach for standing purposes. For example:

***Credential Stuffing & Account Takeovers.*** Mr. O'Neill opines that armed with a "Comcast username, email, and cracked password," hackers can access a victim's internal Comcast account, providing access to stored personal data like payment card information. Ex. C, O'Neill Decl. ¶ 23. Furthermore, attackers can use those same credentials to access other personal accounts using the same username and password combination. *Id.* This allows bad actors to access personal data, make fraudulent purchases/withdrawals, and change account settings. *Id*. This supports the allegations of Plaintiffs Andros and Prescott about fraudulent charges on their debit cards/bank accounts used to make payments to Comcast.[14] Mr. O'Neill's opinions also align with the experience of Plaintiffs Birnie (Ex. H, Birnie Decl. ¶ 9: fraudulent purchases on other personal

[14] Steven Prescott is an authorized user on the Kathleen Wise account.

accounts); Durham (Ex. I, Durham Decl. ¶ 11: unauthorized access to bank account and changing of account settings); Estevez (Ex. J, Estevez Decl. ¶¶ 13-14: fraudulent withdrawals and charges on financial accounts and access of other personal accounts); Fail (Ex. K, Fail Decl. ¶ 11: fraudulent charges on bank account statement); and Nanez (Ex. M, Nanez Decl. ¶ 10: unauthorized attempted access into the Roblox account used to monitor her child). *See also Greek Islands Cuisine, Inc.*, 2024 WL 5223144, at *4 (finding standing when the plaintiffs alleged that the last four digits of a social security number could be used in combination with a name to access existing accounts).

***Phishing & Social Engineering Attacks.*** Mr. O'Neill also opines that using a combination of name, phone, email address, physical/billing addresses, customer ID/account numbers and phone numbers, attackers could craft targeted phishing or social engineering schemes. Ex. C, O'Neill Decl. ¶ 23. These schemes attempt to trick victims into revealing more sensitive information (*e.g.*, login credentials) or convincing them to engage in a host of activities against their interests. *Id.* For example, attackers can send convincing phishing emails pretending to be Xfinity or Comcast. Additionally, this information can be used to text or call pretending to be a customer service representative to extract more sensitive information or commit more fraud and identity theft. *Id.* These opinions support the allegations of Smith (Ex. P, Smith Decl. ¶ 8: targeted and sophisticated Xfinity/Comcast phishing and social engineering attacks); and Estevez (Ex. J, Estevez Decl. ¶ 12: call from someone purporting to be a Comcast customer service representative).

***Sim Swapping & Port-Out Fraud.*** Mr. O'Neill opines that with a combination of PII, such as address, date of birth, last four digits of Social Security number, passwords, and so on, bad actors may be able to con the victim's phone company into believing the request to port out the

number is from the authorized account holder. Ex. C, O'Neill Decl. ¶ 23. If successful, the bad actor can access the victim's accounts, including bank account. *Id.* This is precisely what happened to Plaintiff Estevez. FACC ¶¶ 57-59; Ex. J, Estevez Decl. ¶ 12.

In addition, Mr. O'Neill opines on the last four digits of one's Social Security number. A partial Social Security number is used by companies to authenticate an individual. Ex. C, O'Neill Decl. at ¶ 16. Thus, with the last four digits, a bad actor can pose as a victim like Plaintiff Estevez to verify themselves to Comcast or gain access to other accounts. *See also Greek Islands Cuisine, Inc.*, 2024 WL 5223144, at *4 (finding standing when the plaintiffs alleged that the last four digits of a social security number could be used in combination with a name to access existing accounts). Furthermore, Mr. O'Neill opines that it is not uncommon for bad actors to combine the last four digits of a Social Security number with other public or semi-public data to determine one's date of birth, for example. Ex. C, O'Neill Decl. ¶¶ 16, 19. With this information, malicious actors can reconstruct the full Social Security number. *Id.*

Accordingly, "but for" Comcast's inadequate data security practices, Plaintiffs' data would not have been compromised, and they would not have experienced the alleged instances of fraud and identity theft that Mr. O'Neill explains is connected to that data. *See Tignor v. Dollar Energy Fund, Inc.*, 745 F. Supp. 3d 189, 196-97 (W.D. Pa. Aug. 15, 2024) (finding the plaintiffs' "PII could not have been exfiltrated in the Data Breach 'but for' Dollar Energy's failure to safeguard it….[a]t the pleading stage, the Court finds that Plaintiffs have alleged sufficient facts to establish traceability."). Defendants cite no case in this or any other circuit that suggests Plaintiffs must disambiguate the harm that may have been caused by other data breaches—that is Defendants' burden at summary judgment or trial. *See also Remijas*, 794 F.3d at 696 (emphasizing that where "multiple companies . . . could have exposed the plaintiffs' private information to the hackers, then

the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the but-for cause of the plaintiff's injury") (citation omitted).

Comcast's factual attack on traceability must fail.

2. Citrix's facial attack on traceability fails.

Citrix's challenge to traceability suffers a similar fate. Citrix raises a handful of arguments for its contention that the causal link between Plaintiffs' injuries and Citrix is broken. Each one fails.

Here, Plaintiffs plausibly allege that injury and risk of additional future harm is clearly traceable to the Data Breach and specifically challenged Citrix's conduct because, as detailed in the FACC, Citrix provided Comcast with defective software containing serious vulnerabilities, enabling the hackers to ultimately acquire Plaintiffs' information. FACC ¶¶ 1-4, 8, 306. Plaintiffs also allege how Citrix failed to adequately test the security of its NetScaler Products and that it knew or should have known that its NetScaler Products, which provided access to Comcast's networks, were actively being exploited, and took months to reveal the vulnerability to Comcast. *Id.* at 306-309. When Citrix finally did, it downplayed the severity of the vulnerability. *Id.* Had Citrix adequately tested its NetScaler Products, monitored their performance, and provided Comcast with timely information about the severity of the vulnerability, the Data Breach would not have occurred or would have been substantially mitigated. *Id.* at 486. This but-for causation allegation satisfies traceability for pleading purposes: "but-for" Citrix's specifically alleged negligence, the Plaintiffs would not have been damaged in the breach. *Id.* at 306, 321, 342. *See Tignor*, 745 F. Supp. 3d at 196-97. The same is true for data breaches where a vendor, who may lack direct relationship with the consumers, causes the breach by its own actions or inactions. *See In re MOVEit Customer Data Sec. Breach Litig.,* No. 1:23-MD-03083-ADB-PGL, 2024 WL

5092276, at *12 (D. Mass. Dec. 12, 2024) (refusing to dismiss data breach case where "claim that adequate vendor/third-party risk management . . . would have prevented the Data Breach" adequately alleged at the pleading stage that the plaintiffs' injuries are traceable to those parties).

Citrix's challenge to traceability also fails because it improperly conflates traceability with proximate cause, arguing that Plaintiffs cannot show traceability because Plaintiffs provided their PII to Comcast, that Comcast oversaw installing the Citrix Bleed patch and had insufficient security procedures, [redacted] In doing so, Citrix ignores the facts supporting the causal link between Citrix and the breach—its software was defective, it failed to timely find the Citrix Bleed vulnerability, it took months for Citrix to discover the vulnerability (by which time it was being exploited), and it was forced to supplement the patch information to make clear to "kill[] all active and persistent sessions" by which time the Data Breach had already begun. This alone is sufficient to reject Citrix's traceability challenge.

As a threshold matter, Citrix improperly overlays a proximate cause standard on the traceability prong of Article III. *See Lexmark Intern., Inc.* 572 U.S. at 134 n.6 ("Proximate causation is not a requirement of Article III standing, which only requires that the plaintiff's injury be fairly traceable to the defendant's conduct."). Moreover, lack of prior *direct* relationship with the affected victim also does not defeat the "but-for" causal link, and *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451 (D.N.J. 2013)—Citrix's main case—does not stand for such a broad proposition. The issue with *Polanco* was not solely lack of direct relationship, but that the defendant "was not involved in any way [at all] in [the] specific chain of events," that lead to the loss of the plaintiff's data, which is not the case here. *Polanco*, 988 F. Supp. 2d at 465. Here, Plaintiffs clearly allege how Citrix's defective software and its continuing failure to detect or patch

the Citrix Bleed vulnerability enabled cybercriminals to steal Plaintiffs' PII from Comcast. FACC ¶¶ 2-5, 306-313. Simply put, Citrix handed cybercriminals with the digital keys to Comcast's data-rich kingdom. *Id.* at 8-9. *LaSpina*, 985 F.3d at 287 ("[S]tanding may be satisfied even if the plaintiff alleges an indirect (or multistep) causal relationship between the defendant's conduct and her injury.").

Citrix also cannot escape liability by arguing that Comcast delayed implementing software patch, especially considering that Citrix failed to adequately communicate the severity or of the vulnerability or proper implementation of the patch when initially sent to Comcast. Accepting Citrix's argument ignores Citrix (1) failing to find the Citrix Bleed vulnerability for months after its initial active exploitation, and (2) failing to make clear the importance of the patch by identifying that the vulnerability had taken place, or that more importantly, Comcast would need to "kill[] all active and persistent sessions" to ensure security of the network. FACC ¶ 309. But either but-for causation *or* concurrent causation may satisfy traceability, and both Comcast and Citrix can be held responsible for the Data Breach as joint tortfeasors. *Clemens*, 48 F.4th at 158. ("we have held that but-for causation is sufficient to satisfy traceability"); *see also Remijas*, 794 F.3d at 696 ("If there are multiple companies that could have exposed the plaintiffs' private information to the hackers, then the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the but-for cause of the plaintiff's injury.") (cleaned up), citing *Price Waterhouse v. Hopkins*, 490 U.S. 228, 263 (1989) (O'Connor, J. concurring).

[redacted] Comcast's security measures

would not have been challenged if Citrix's products hadn't been initially vulnerable and any vulnerabilities by Comcast [redacted] do not excuse Citrix's negligence or release it from its duty to the Plaintiffs. *Roma*, 2024 WL 3678984, at *7 ("Either but-for causation or concurrent causation can establish a legally sufficient relationship between the injury-in-fact and the challenged conduct."). Plaintiffs are not required to show that Citrix, *and only Citrix*, is responsible for the breach, only that their damages are traceable, at least in part, to Citrix. *See In re Am. Med. Collection Agency Customer Data Sec. Breach Litig.*, 2021 WL 5937742, at *12 (D.N.J. Dec. 16, 2021) ("the participation of third parties does not defeat traceability where, as here, a plaintiff alleges facts suggesting a nonspeculative causal link."); *see also Attias v. CareFirst, Inc.*, 431 U.S. App. D.C. 273, 282, 865 F.3d 620, 629 (2017) ("Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires only that those injuries be 'fairly traceable' to the defendant").

*In re MOVEit Customer Data Sec. Breach Litig* is also instructive. There, multiple parties were all allegedly responsible for a massive data breach, at least in part. A number of "Vendor Contracting Entities" moved to dismiss the complaint, arguing "that because the cyberattack targeted Vendors' servers, and not the servers of the [Vendor Contracting Entities], 'no amount of cybersecurity by these Defendants . . . could have prevented the MOVEit Incident[] from occurring.'" *In re MOVEit*, 2024 WL 5092276, at *12. This is similar to Citrix's argument here: that because the Data Breach took place on Comcast's and Effectv's servers and it provided a patch, it cannot be held liable. This argument should be rejected, as the court did in *MOVEit*. As the *MOVEit* court explained "Plaintiffs' injuries are fairly traceable, at least in part, to the actions of those parties," and further held that "Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires only

that those injuries be 'fairly traceable' to the defendant." *Id.* at *78-79. The same is true here.

Citrix also cannot contradict Plaintiffs' well-pled allegations at this stage. *See* ECF No. 161 at 12 (contending that "NetScaler is not designed be, and Citrix does not advertise or market it to be, data storage of (sic) data transfer software"); *Cf.* FACC ¶¶ 236-238 (pleading that Citrix "knew that its NetScaler Products would be used by companies like Comcast to provide a secure remote connection" but Citrix failed to ensure that this software was secure, and thus, enabled access by hackers). By allowing users to secure, hold, and transmit PII through its software, the traceability link is not broken by the virtue of existence of foreseeable third-party actor, like a hacker. Thus, Citrix's failure to secure its software and its delayed, inadequate communication about the Citrix Bleed vulnerability and security patch directly contributed to the Data Breach. FACC ¶¶ 236-237.

Finally, Citrix argues that "the Amended Complaint identifies multiple other instances when Comcast customer data was posted to the dark web, which further attenuates any connection between Citrix and Cloud SG (or even the Comcast Data Incident) and Plaintiffs' purported injuries." ECF No. 161 at 15. Citrix's argument, which it is free to raise at trial, has been rejected by other courts at the pleading stage. *See Roma*, 2024 WL 3678984 at *9 ("the injuries that Plaintiffs allege have an established pedigree in tort cases arising out of data breaches. Courts in both California and Pennsylvania have found that injury by way of costs relating to credit monitoring, identity theft protection, and penalties can sufficiently support a negligence claim) (cleaned up); *see also Gaddy v. Long & Foster Cos.*, No. CV 21-2396 (RBK/SAK), 2022 WL 22894854, at *7 (D.N.J. Mar. 15, 2022) (holding that sensitive nature of the information stolen and temporal proximity between data breach and unauthorized credit activity permit inference the breach was the cause); *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633 (N.D. Cal. 2020) ("the mere

fact that Plaintiff has been a victim of other more serious breaches in the past does not mean a substantial connection between this breach and her decision to monitor her credit more closely is lacking. Defendant does not get a free pass on this basis.") (cleaned up); *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011) ("If there are two alternative explanations, one advanced by defendant and the other advanced by plaintiff, both of which are plausible, plaintiff's complaint survives a motion to dismiss under Rule 12(b)(6).").

Accordingly, Plaintiffs have met their pleading burden to show that their injuries are traceable to Citrix.

**C. Plaintiffs have standing to seek declaratory and injunctive relief.**

Comcast claims Plaintiffs cannot seek declaratory and injunctive relief because their injuries lack redressability. ECF 158-2 at 34.[15] But as set forth in the FACC, Plaintiffs require declaratory and injunctive relief to redress their imminent risk of harm.

To establish standing for declaratory or injunctive relief, Plaintiffs must show "a favorable decision from the court is likely to redress their alleged injury." *Richard Roe W.M. v. Devereux Found.*, 650 F. Supp. 3d 319, 334 (E.D. Pa. 2023). Redressability requires a plaintiff to show that they "personally would benefit in a tangible way from the court's intervention." *Id.* (internal citation omitted). Specifically, "for legal or equitable relief, a favorable opinion need not relieve every injury; the judgment need only relieve a 'discrete injury.'" *Lutter v. JNESO*, 86 F.4th 111, 128 (3d Cir. 2023) (internal citation omitted). But the declaratory judgment must "completely resolve[ ] a concrete controversy susceptible to conclusive judicial determination." *Id.* Plaintiffs have satisfied these standards.

[15] Comcast is the only defendant to challenge redressability, and it does so only as to Plaintiffs' request for declaratory and injunctive relief.

As to Plaintiffs' request for declaratory relief, the Declaratory Judgment Act provides that "[i]n a case of actual controversy within its jurisdiction, . . . any court of the United States . . . may declare the rights and legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought." 28 U.S.C. § 2201(a). The underlying controversy here is whether Defendants' data security measures are sufficient to protect Plaintiffs and Class Members from further data breaches compromising their PII. FACC ¶ 503. Plaintiffs allege that Defendants' data security measures remain inadequate, and, as a result, Plaintiffs and Class Members continue to suffer injury because they remain at imminent risk of further compromises of their PII. *Id.* Plaintiffs seek an entry of judgment that Defendants owe Plaintiffs legal duties under both common and statutory law and that Defendants continue to breach these duties by failing to employ reasonable data security measures to safeguard Plaintiffs' PII stored in Comcast's system. *Id.* at ¶ 504. A judgment on these two requests would "be of significant practical help in ending the controversy." *Butta v. GEICO Cas. Co.*, 400 F. Supp. 3d 225, 231 (E.D. Pa. 2019) (citing *Step-Saver Data Sys. v. Wyse Tech.*, 912 F.2d 643, 650 (3d Cir. 1990)). Thus, this "falls within the traditional scope of declaratory judgment actions because it completely resolve[s] a concrete controversy susceptible to conclusive judicial determination." *Calderon v. Ashmus*, 523 U.S. 740, 749 (1998).[16]

Plaintiffs' requested injunctive relief would also redress their injuries because "the injunction proposed by plaintiffs would change the systemic conditions that place them in danger of abuse." *Richard Roe W.M.*, 650 F. Supp. 3d at 335 (citing *Massachusetts v. EPA*, 549 U.S. 497, 526 (2007)). Plaintiffs allege that Defendants failed to fully comply with industry-standard

[16] Comcast's other argument, that courts have rejected claims for declaratory judgment where they are duplicative, has little to do with standing and is addressed below in Plaintiffs' discussion of the sufficiency of their claim under the Declaratory Judgment Act.

cybersecurity practices, including the following:

> [redacted] setting up proper network segmentation, using secure credential storage rather than storing PII in plain text, engaging in user-activity monitoring, ensuring data-loss prevention, conducting vigilant monitoring for and timely patching vulnerabilities, deploying comprehensive intrusion detection and prevention systems, failing to train and audit employees on basic cybersecurity practices, failing to provide full and complete patching guidance before publicly announcing the vulnerability, failing to adequately test, secure, and monitor the Citrix NetScaler Products, and retaining PII even after a customer terminates Comcast's services."

FACC ¶¶ 351. Plaintiffs also allege that Comcast stores former customers' PII for an indefinite period after they terminated their services. *Id.* at ¶ 188. Thus, requiring Comcast to "delete, destroy[,] and purge the PII of Plaintiffs and Class Members," engage independent third-party security auditors, and conduct internal training and education programs regarding data security will achieve systemic changes to the conditions placing Plaintiffs and Class members in danger of harm. Furthermore, to the extent Comcast still uses Citrix's NetScaler Products, a repeat of Citrix's failures here would expose Plaintiffs—again—to significant consequences. That the Data Breach already occurred ignores the potential for new exposures of Plaintiffs and Class Members' PII should Defendants fail to remain vigilant in their cybersecurity practices. Plaintiffs want Defendants to implement and maintain industry-standard cybersecurity practices to prevent further disclosures of Plaintiffs' PII. *See* Ex. G, Andros Decl. ¶ 19; Ex. H, Birnie Decl. ¶ 17; Ex. I, Durham Decl. ¶ 19; Ex. J, Estevez Decl. ¶ 23; Ex. K, Fail Decl. ¶ 20; Ex. L, Hendrickson Decl. ¶ 17; Ex. M, Nanez Decl. ¶ 17; Ex. N, Nunn Decl. ¶ 15; Ex. O, Prescott Decl. ¶ 19; Ex. P, Smith Decl. ¶ 15; Ex. Q, Verdier Decl. ¶ 19; Ex. R, Wilson Decl. ¶ 14; Ex. S, Wolfson Decl. ¶ 16.

Thus, because the requested declaratory and injunctive relief is prospective, it will provide

an actual benefit, and redress Plaintiffs' injuries, Plaintiffs have standing to request such relief.

## V. IF THE COURT FINDS PLAINTIFFS DO NOT HAVE ARTICLE III STANDING, THEN IT MUST REMAND THIS LITIGATION TO STATE COURT.

Without any legal support, Defendants have repeatedly represented to the Court that it may grant Defendants' motions and dismiss Plaintiffs' claims with prejudice. *See* ECF No. 158-2 at 5 ("… Plaintiffs' FACC must be dismissed in its entirety and with prejudice."); ECF No. 184 at 1 ("… Defendants continue to request that the Court dismiss this action with prejudice for lack of Article III standing."). This is false. It is a universally accepted legal maxim that where the Court lacks subject matter jurisdiction, it lacks the power to adjudicate the merits of those claims. *See In re Orthopedic "Bone Screw" Prods. Liab. Litig.*, 132 F.3d 152, 155 (3d Cir. 1997) ("If a court then determines that it lacks subject matter jurisdiction, it cannot decide the case on the *merits*. It has no authority to do so. A federal court can only exercise that power granted to it by Article III of the Constitution and by the statutes enacted pursuant to Article III."). Thus, if the Court determines it lacks subject matter jurisdiction, the appropriate step is to remand the action to state court. *See Bloom v. Barry*, 755 F.2d 356 (3d Cir. 1985).

To the extent the Court determines that some or all Plaintiffs do not have Article III standing to sue in federal court, Plaintiffs' Counsel have filed state court actions in California (*Scheirer v. Comcast Cable Communications LLC et al.*, No. 2001016688 (Ca. Super. Ct. Alameda Cty.) and Pennsylvania (*Emmett v. Comcast Cable Communications LLC et al.*, No. GD-25-003268 (Pa. Ct. Com. Pleas Allegheny Cty.) to serve as placeholders where this case can be remanded to state court to proceed without delay. Despite Defendants' pending motions seeking to establish that this Court lacks subject matter jurisdiction, Defendants removed the state court cases taking the position that the federal courts have subject matter jurisdiction over those claims and injuries arising from the Data Breach. This practice is dubious at best, especially here when

Citrix argues the same allegations here are facially implausible to provide Article III standing. These two positions cannot be reconciled. *See Fidelity & Deposit Co. of Md.*, 653 F.2d at 777 (deciding that statements made by a party "in connection with other litigation that is adverse to, or inconsistent with, its position in this case . . . is admissible as evidence against" that party).

## VI. PLAINTIFFS ADEQUATELY ALLEGE CITRIX'S NEGLIGENCE (COUNT 7).

To state a claim for negligence against Citrix, Plaintiffs must allege duty, breach, a causal connection between the breach and resulting injury, and damages. *Jones v. Plumer*, 226 A.3d 1037, 1039 (2020). Citrix asserts that it has no duty to Comcast's customers arising from Comcast's use of its software to store and protect customer PII, and that its actions were not the cause of Plaintiffs' injuries. But Citrix's duty to Plaintiffs and other Comcast customers is rooted in longstanding principles of negligence law. And Citrix's failure to adequately detect and remedy vulnerabilities in its products, together with Comcast's actions, were a proximate cause of the actual injuries suffered by Plaintiffs and other members of the putative class. *See Harsh v. Petroll*, 887 A.2d 209, 218 (Pa. 2005) ("Pennsylvania tort law also maintains that multiple substantial factors may cooperate to produce an injury . . . and that concurrent causation will give rise to joint liability."). Plaintiffs have therefore alleged a viable claim for negligence against Citrix.

### A. Citrix Had a Duty to Protect Comcast Customers' PII.

Under Pennsylvania law, the existence of a duty is a question of law. *Maghakian v. Cabot Oil & Gas Corp.*, 171 F. Supp. 3d 353, 359 (M.D. Pa. 2016); *In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 526 (M.D. Pa. 2021). A straightforward application of Pennsylvania negligence principles demonstrates that Citrix owed a duty to Plaintiffs to safeguard their PII. Preliminarily, Citrix's argument that only entities that collect or possess individuals' PII owe a duty in a data breach context overstates the law. Negligence claims in the data breach context are not so limited, and an entity does not need to collect individuals' sensitive data to owe a duty of

care. Instead, a duty of care may also generally arise based on an actor's affirmative conduct and the risk of foreseeable harm. *In re Rutter's*, 511 F. Supp. 3d at 528-29 (M.D. Pa. 2021) (citing *Dittman v. UPMC*, 196 A.3d 1036, 1047 (2018)) ("we understand *Dittman* to support a more general principle that has significant applicability here—that in new factual scenarios, a court need not undertake the burdensome task of carving out new legal duties, but, instead, courts can and should apply longstanding duties").[17]

Where an actor's affirmative conduct creates the risk at issue, that actor's duty is generally presumed. *Dittman*, 196 A.3d at 1047; *see also* Restatement (Second) of Torts § 302 cmt. a (1965) ("In general, anyone who does an affirmative act is under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act."). This concept is supported by "longstanding jurisprudence" in Pennsylvania. *In re Rutter's*, 511 F. Supp. 3d at 529. Here, Citrix's affirmative conduct arose from two sets of actions by Citrix.

First, Citrix affirmatively created a line of products that it intended would be used to, among other uses, safeguard sensitive information and manage authentication for its customers. FACC ¶¶ 209-13, 215-16, 230. For instance, Citrix notes on its website that "[r]esponsibly adopting advanced technologies requires a critical eye on cybersecurity and data privacy. Because we design our products around centralized delivery, visibility and control of apps and data, security is built into the core of our solutions and practices." *Id.* at ¶ 217. Citrix also offered maintenance

[17] Citrix cites a handful of cases to support its contention that a duty can *only* exist where a defendant collected or had possession of sensitive information. *See, e.g.*, *Kroeck v. UKG, Inc.*, No. 2:22-CV-66, 2022 WL 4367348 (W.D. Pa. Sept. 21, 2022); *In re Rutter's*, 511 F. Supp. 3d at 527; ECF No. 161, at 17-18. But the cherry-picked language to which Citrix cites arose from context of the cases at issue and does not delineate, and do not stand for a brightline rule outlining the *only* way a duty can arise in data breaches. Instead, these cases emphasize the broad, general principle (applicable in an array of data breach scenarios) that a defendant owes data breach victims a duty where the defendant's "affirmative conduct had created a foreseeable risk of data breach." *See In re Rutter's,* 511 F. Supp. 3d at 527.

and support for these products for all of its customers, and as demonstrated by its creation of a patch for the Citrix Bleed vulnerability, Citrix recognized that its customers would rely on Citrix to protect the security of its products. *See id.* at ¶¶ 4, 310-12. This is sufficient to establish a duty to individuals, like Plaintiffs, who would likely experience harm if Citrix failed to ensure the integrity and security of its products. *See Batchelar v. Interactive Brokers, LLC*, 422 F. Supp. 3d 502, 515 (D. Conn. 2019) (concluding that a software designer had duty to exercise reasonable care when "designing, testing, and maintaining software," where it was foreseeable that "failure to use care might result in a flaw in the software that could cause the specific type of harm claimed by [plaintiff] here," and collecting similar cases from several states applying general duty principles).

Second, Citrix publicized to everyone (including cybercriminals) the existence of a critical vulnerability in its products *before* providing customers, like Comcast, with complete mitigation guidance. Citrix initially announced the existence of Citrix Bleed on October 10, 2023. *Id.* at ¶ 281. In the initial announcement, Citrix included a detailed explanation of how Citrix Bleed could be exploited to hijack user sessions and gain access to customers' secure systems. *Id.* at ¶ 281 n.92. As part of this announcement, Citrix provided a "patch" that customers could install on their systems. *Id*. But the "patch" and related guidance that Citrix released as part of the October 10 announcement was insufficient to fully mitigate exploits of Citrix Bleed, because the patch would not terminate any user sessions that were hijacked *prior* to the installation of the patch. *Id.* at ¶¶ 309-10. Citrix did not provide full and complete mitigation guidance to customers until nearly *two weeks later*, when it finally communicated to customers that fully "patching" Citrix Bleed required customers to "kill" (*i.e.*, reset) all active user sessions. *Id*. Citrix withheld this critical information for thirteen days, even though cybercriminals often exploit vulnerabilities to steal information from

companies' systems as soon as 15 minutes after they are announced. *Id.* at ¶ 288. Courts do not hesitate to find a duty where an actor's affirmative conduct so clearly subjects foreseeable victims to such a clear risk of harm. *See, e.g.*, *Dittman*, 196 A.3d at 1046; *Feld v. Merriam*, 485 A.2d 742, 746-47 (Pa. 1984) (holding that landlord may have assumed duty to protect tenants when it undertook to provide secured parking and knew tenants would rely on it to keep parking area safe). Likewise here, Citrix's conduct in announcing the Citrix Bleed vulnerability without providing full mitigation guidance created an unreasonable risk that cybercriminals would exploit the vulnerability and steal customers' confidential data, including Plaintiffs' and Class Members' PII stored in Comcast's databases. *See id.* at ¶ 233.

Citrix's public statements further reinforce Citrix's duty, demonstrating that Citrix *knows* that its products are used to manage highly sensitive information and is aware of the foreseeable risk of data breaches that exploit vulnerabilities in its products should it not uphold its duty. *See id.* at ¶ 215. For example, Citrix's "Trust Center" markets its ability to keep customers' data secure, stating that is customers "have trusted our ability to handle their data with care and respect" and emphasizing that Citrix's ability to protect sensitive data has led to "organizations from the most highly regulated sectors rely on us to protect their most sensitive information wherever work happen." *Id.* at ¶ 217. Similarly, Cloud Software Group's privacy statement states that the company and its subsidiaries (such as Citrix) protect personal information by "maintain[ing] administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of Personal Information." *Id.* at ¶ 219. And in its 2021 10-K Annual Report, Citrix states that unauthorized parties may attempt to compromise confidential information of its customers or their end users and that this may result in individual and/or class action lawsuit. *Id.* ¶ 215. Overall, Citrix's marketing and public statements demonstrate that Citrix knew its products were used to

protect and manage access to sensitive PII, and became attractive targets for cybercriminals as a result. *Id.* at ¶ 230. In circumstances where a defendant is so plainly aware of a risk that its conduct created, courts do not hesitate to find the existence of a duty. *See Mahan v. Am-Gard, Inc.*, 841 A.2d 1052, 1061 (Pa. Super. 2003) (citing *Ford v. Jeffries*, 379 A.2d 111, 115 (Pa. 1977)) ("Where a risk is this foreseeable, an actor may be held liable where that party 'realized or should have realized the likelihood that such a situation might be created and that a third person might avail himself of the opportunity to commit such a tort or crime.'").[18]

In an attempt to muddy the waters of these straightforward legal principles, Citrix cites a litany of case law that address fundamentally distinct circumstances from a data breach and are inapposite to the facts of this case. *Fragale v. Wells Fargo Bank, N.A.*, for example, involved a plaintiff seeking to hold a bank liable for failing to prevent a fraudulent wire transfer. 480 F. Supp. 3d 653 (E.D. Pa. 2020). And *Zanine v. Gallagher* addressed a police officer attempting to establish causation between his heart attack and the high-speed chase in which he took part. 497 A.2d 1332 (Pa. Super. Ct. 1985). Both cases address circumstances that are a far cry from the subject of data breaches, and unlike the present case, involved risks that were not reasonably foreseeable to the defendants. Indeed, the foreseeability of a heart attack during a high-speed chase and the foreseeability that hackers may try to breach systems containing sensitive PII using Citrix's software are hardly analogous.

Conversely, the data breach cases that Citrix tries to distinguish to argue that Citrix owed

[18] [redacted]

no duty to Plaintiffs are far more comparable to the facts of this case than what Citrix suggests. The court in *In re Accellion, Inc. Data Breach Litigation*, for example, found that a company that produced file transfer software owed a duty to individuals whose data was transmitted using the company's software. 713 F. Supp. 3d 623, 635 (N.D. Cal. 2024). In reaching that conclusion, the court rejected the defendant's argument that it "lack[ed] contractual privity with Plaintiffs and played no role in how Plaintiffs' information was provided or used by its clients." *Id.* at 634. The court also relied partly on the plaintiffs' allegations that the defendant was "in the position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class members from a resulting data breach," and further noted that the defendant demonstrated its control over the plaintiffs' data when it released patches to fix the vulnerabilities that were exploited in that data breach. *Id.* Likewise here, Citrix was in a key position to protect its software from the foreseeable risk of a data breach that would endanger Plaintiffs' and class members' PII, as evidenced by the critical role that Citrix had in producing a patch after the Citrix Bleed vulnerability was discovered. FACC ¶¶ 4, 211. Although *Accellion* applied California legal principles to reach its conclusion, the factual scenario in that case is not nearly as different as Citrix claims. Indeed, although Citrix claims that NetScaler Products are "updated" and "managed" by the customer (*i.e.*, Comcast) rather than Citrix, Citrix's public statements about its role in maintaining the security of its products suggests otherwise. *See, e.g.*, FACC ¶¶ 211, 217-24.

Overall, Citrix seeks to exploit the novelty of the factual scenario present in this case to distract from the obvious application of a longstanding and well-established duty. But as the Pennsylvania Supreme Court has recognized:

> [I]t is unnecessary "to conduct a full-blown public policy assessment in every instance in which a longstanding duty imposed on members of the public at large arises in a novel factual scenario." Common-law duties stated in general terms are framed in such fashion for the very reason that they have broad-scale application.

*See Dittman*, 196 A.3d at 1046 (quoting *Alderwoods (Pennsylvania), Inc. v. Duquesne Light Co.*, 106 A.3d 27, 40 (2014)). Despite Citrix's implication that the law in this area is unsettled and unresolved, basic principles of duty under Pennsylvania law are straightforward. When applied in this case, those principles dictate a finding that Citrix owed Plaintiffs a duty to safeguard the PII that was stored using Citrix products.

**B. Citrix's Breach of Its Duty Caused Plaintiffs' Injuries.**

Citrix further alleges that Plaintiffs fail to plead that Citrix proximately caused Plaintiffs' injuries, as Citrix claims there is only a remote causal connection between Citrix's actions and the harm that Plaintiffs experienced. But Citrix played a central and substantial role in the data breach and Plaintiffs' resulting injuries, and Citrix's relationship to Plaintiffs' harms is anything but remote.

As set forth above, proximate cause under Pennsylvania law is a determination of "whether the alleged negligence was so remote that as a matter of law, the defendant cannot be held legally responsible for the subsequent harm." *Holt v. Navarro*, 932 A.2d 915, 921 (Pa. Super. Ct. 2007). Where a defendant's actions are a "substantial factor" in causing harm, however, the defendant can be held liable. *See Heeter v. Honeywell Int'l, Inc*., 195 F. Supp. 3d 753, 758 (E.D. Pa. 2016). To determine whether a defendant's actions are a "substantial factor," Pennsylvania courts generally look to the factors set forth in the Restatement (Second) of Torts, including the number of other factors contributing to the harm, whether a defendant's conduct created a force or series of forces which are in continuous and active operation up to the time of the harm, and lapse of time. *Holt,* 932 A.2d at 921. Questions of proximate case are typically reserved for the jury, *Summers v. Certainteed Corp.,* 997 A.2d 1152, 1163–64 (Pa. 2010), and only where reasonable minds could not differ may a court rule on the issue as a matter of law and remove it from the jury.

*Vanesko v. Marina Dist. Development Co.*, 38 F. Supp. 3d 535, 544 (E.D. Pa. 2014).

Here, a jury could easily conclude that Citrix's cascading failures were a substantial factor in the Data Breach and resulting injuries faced by Plaintiffs and the putative class. Citrix initially failed to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of its NetScaler Products; failed to adequately engage in penetration and vulnerability testing to assess and mitigate these risks; failed to design and implement safeguards to control these risks; and failed to adequately test and monitor the effectiveness of any such safeguards. FACC ¶ 485. Citrix also failed to implement reasonable measures to detect vulnerabilities in its NetScaler Products, as evidenced by actual exploits of the Citrix Bleed vulnerability by hackers at least two months before Citrix ever announced the existence of the vulnerability or a patch for the vulnerability. FACC ¶ 306.

Citrix's negligence did not end after it finally identified the Citrix Bleed vulnerability. Citrix's initial announcement and patch failed to fully communicate the severity of the vulnerability. *Id.* at ¶ 309. Indeed, Citrix's communications to Comcast may have even downplayed the severity of the issue, due to concerns that the vulnerability may damage a potential business deal with a different Comcast business division. *Id*. at ¶¶ 8, 311. And while Citrix originally recommended that NetScaler customers only needed to install a software "patch" to fix the Citrix Bleed vulnerability from their products, Citrix waited until two weeks later to communicate that customers needed to "kill" all active user sessions to fully halt exploits of Citrix Bleed. *Id.* at ¶ 309. In sum, Citrix failed to take proper mitigating action once it discovered the Citrix Bleed vulnerability, and Citrix failed to adequately communicate the severity of the breach to its customers.

These failures, particularly Citrix's failure to timely detect, properly respond to, and

provide complete mitigation guidance regarding the NetScaler vulnerability created a force that was in continuous operation up until the harm suffered by Plaintiffs. As Citrix itself recognizes, its enterprise customers heavily rely on Citrix to protect their sensitive data from breaches and other security risks. *See* FACC ¶¶ 217-19. Its customers therefore relied on Citrix to timely identify vulnerabilities like Citrix Bleed, and if such a vulnerability was discovered, to timely and adequately rectify such a vulnerability. But here, Citrix failed to alert customers to Citrix Bleed's existence until at least two months after cybercriminals were exploiting the vulnerability. *See id.* ¶¶ 211-13, 217. Citrix's initial announcement about the vulnerability on October 10, 2023, further failed to alert its customers to the severity of the breach, *id.* ¶ 309, which likely caused its customers to act less expediently in instituting Citrix's patch. Moreover, the patch that Citrix released on October 10 failed to completely repair the vulnerability in Citrix's products, as nearly *two weeks later* Citrix released additional guidance that NetScaler customers needed to end all active user sessions in order to fully mitigate risks arising from Citrix Bleed. *Id.*[19] Citrix's failures therefore created a situation where a risk of harm (a data breach) was nearly inevitable; it was not, as Citrix suggests, harmless absent "myriad causative factors." ECF No. 161, at 29.

Additionally, there is minimal lapse in time between Citrix's negligence and the data breach that resulted from that negligence. This Court has previously held that "[l]apse of time alone is not sufficient to prevent an actor's negligence from being the proximate cause of a harm."

[19] Citrix claims that the FACC is contradictory on the adequacy of Citrix's initial patching guidance. *See* ECF No. 161, at 24. Not so. As explained in the FACC and herein, Citrix's initial patch *did* offer sufficient guidance for its customers to prevent future exploits of the vulnerability. FACC ¶¶ 306-13. But if cybercriminals had *already* hijacked user sessions by exploiting the vulnerability before a customer could install that initial patch, as occurred with Comcast, customers' systems were not fully secured and patched until they complied with Citrix's October 23 guidance and killed all active user sessions. *Id.* Given that cybercriminals could have exploited Citrix Bleed within minutes of Citrix's public announcement on October 10, FACC ¶ 288, it was negligent for Citrix to not provide that complete guidance until nearly two weeks later.

*Heeter*, 195 F. Supp. 3d at 761. The lapse of time between Defendant's release of the NetScaler patch and Comcast's implementation thereof does not preclude a finding that Defendant proximately caused Plaintiffs' harm. Rather, "it is to be weighed alongside the other considerations set forth in the Restatement [of Torts]." *Id.* Defendants cannot use the lapse in time to justify the dismissal of the entire claim.

Certainly, as Citrix highlights, Comcast bears some liability for Plaintiffs' injuries. As set forth in the FACC, Comcast failed to implement appropriate security measures to monitor and secure its own systems, [redacted] and other measures. *See* FACC ¶ 303; *see also* ECF No. 161, at 28-30. Comcast also failed to discover the theft of Plaintiffs' and Class Members' PII in a timely manner, [redacted]. *See* FACC ¶¶ 290-95. But if Citrix had properly prevented access to Comcast's systems by cybercriminals in the first place, these internal measures at Comcast would have been irrelevant. If Citrix had adequate protocols in place to detect the Citrix Bleed vulnerability in a timely manner, exploits of Citrix Bleed may never have occurred, and the Data Breach may have been prevented entirely. FACC ¶¶ 287, 306. If Citrix had communicated the need to patch the vulnerability on October 10 with sufficient urgency, Comcast may have patched its systems before cybercriminals began hijacking employees' user sessions on October 16, preventing any unauthorized access to its customers' PII from ever occurring. And if Citrix had provided full mitigation guidance addressing the need to kill all active user sessions earlier than *two weeks* after releasing the initial patch, Comcast could have halted any already-ongoing exploits, mitigating the impacts of the Data Breach or even preventing it entirely.

Citrix's claim that multiple intervening factors disrupt the chain of causation in Comcast's

case ring hollow considering the widespread impact of Citrix's negligence in responding to Citrix Bleed; several large companies beyond Comcast were also hacked through an exploit of Citrix Bleed, including Boeing, Toyota, and the law firm Allen & Overy. FACC ¶ 311. Put simply, absent Citrix's negligent missteps, the Data Breach and theft of Plaintiffs' PII would not have been possible, and Citrix is equally responsible for the resulting harm faced by Plaintiffs.

Just because another party contributed to a harm does not reduce a defendant's own responsibility for their substantial role same harm, *Harsh*, 887 A.2d at 218. Simply pointing to Comcast's own missteps in this case is woefully insufficient for Citrix to extricate itself from its *own* responsibility for the Data Breach and resulting harm to Plaintiffs, particularly at the motion to dismiss stage and prior to full discovery.

## VII. PLAINTIFFS ALLEGE A CLAIM FOR NEGLIGENCE PER SE AGAINST CITRIX (COUNT 8).

Citrix argues that this Court should dismiss Plaintiffs' negligence *per se* claim as "duplicative" of their negligence claim. ECF No. 161, at 31. But courts regularly permit plaintiffs to pursue a negligence *per se* claim as part of their regular negligence claim. *See Weinberg v. Legion Athletics, Inc.*, No. CV 22-1573, 2023 WL 4706165, at *9 (E.D. Pa. July 21, 2023) (stating that where "a plaintiff alleges negligence and negligence per se claims as separate causes of action, courts routinely treat the negligence per se claim as subsumed by the negligence claim."); *see also In re Orthopedic Bone Screw Prod. Liab. Litig.*, 193 F.3d 781, 790 (3d Cir. 1999) (noting that *per se* liability is a separate theory of negligence that "establishes, by reference to a statutory scheme, the standard of care appropriate to the underlying tort"). Thus, Plaintiffs validly plead a separate claim for negligence *per se.* And to the extent the Court finds that Plaintiffs cannot plead this claim separately, the proper remedy, under such circumstances, is not dismissal of the negligence *per se* claim outright, but rather allowing Plaintiffs to pursue their negligence *per se* theory as part of

their negligence claim. *See Roma*, 2024 WL 3678984, at *11 (permitting plaintiffs to press negligence *per se* allegations "as a theory to support their negligence claim"); *In re Rutter's*, 511 F. Supp. 3d at 532 (same).[20]

Citrix further argues that Plaintiffs' negligence *per se* claim should fail because Plaintiffs fail to allege that Section 5 of the FTC Act (on which Plaintiffs base their negligence *per se* claim) even applies to Citrix in the context of the data breach. But Section 5 of the FTC Act is meant to apply broadly, prohibiting all unfair practices "in or affecting commerce." *See* 15 U.S.C. § 45; FACC ¶¶ 432-37. And courts across the country have concluded that Section 5 of the FTC Act can establish a standard of care in data breach matters and give rise to a negligence *per se* claim. *See, e.g.*, *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247 (3d Cir. 2015); *Perry v. Bay & Bay Transp. Servs., Inc.*, 650 F. Supp. 3d 743, 755 (D. Minn. 2023); *First Choice Fed. Credit Union v. Wendy's Co.*, No. 16-cv-506, 2017 WL 9487086, at *4 (W.D. Pa. Feb. 13, 2017). Likewise here, Citrix's "failure to maintain reasonable and appropriate data security" such that it "failed to protect consumers' sensitive personal information can constitute an unfair method of competition in commerce in violation of the Federal Trade Commission Act." *See In re Equifax*, Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019).

This Court should deny Citrix's motion to dismiss Count 8.

## VIII. PLAINTIFFS ALLEGE A CLAIM FOR DECLARATORY JUDGMENT.

The well-pleaded allegations of Plaintiffs' Consolidated Amended Class Action Complaint demonstrate that declaratory relief is warranted and necessary to redress the harm Plaintiffs will

[20] Citrix claims that the law of Plaintiffs' home states would also bar negligence *per se* theories of liability, but cases interpreting the law of these states say otherwise. *See, e.g.*, *In re Accellion, Inc.*, 713 F. Supp. 3d at 639-40; *In re ESO Solutions, Inc. Breach Litig.*, 2024 WL 4456703, at *11 (W.D. Tex. July 30, 2024); *Villazon v. Prudential Health Care Plan, Inc.*, 843 So.2d 842, 852 (Fla. 2003); *Sikora v. Wenzel*, 727 N.E.2d 1277, 1280-82; *Alloway v. Bradlees, Inc*., 723 A.2d 960, 967 (N.J. 1999).

continue to suffer as a result of Comcast's misconduct without such relief.

The Declaratory Judgment Act empowers this Court to enter a judgment declaring the rights and legal relations of the parties and to grant any further necessary relief. *See* 28 U.S.C. § 2201(a). To state a claim for relief under the Declaratory Judgment Act, a plaintiff must adequately allege a dispute that is: (1) "definite and concrete, touching the legal relations of parties having adverse legal interests"; (2) "real and substantial"; and (3) "admit[ting] of specific relief through a decree of a conclusive character, as distinguished from an opinion advising what the law would be upon a hypothetical state of facts." *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 127 (2007). The central question is whether "the facts alleged, under all the circumstances, show that there is a substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality to warrant the issuance of a declaratory judgment*." Id.* at 127 (*quoting Md. Cas. Co. v. Pac. Coal & Oil Co.*, 312 U.S. 270, (1941)).

Plaintiffs have adequately stated a claim for relief under the Declaratory Judgment Act. They allege that the Data Breach leading to the theft of their PII put them at imminent and substantial risk of future fraud, identity theft, and other crimes utilizing their PII, any of which will cause them to incur substantial time and expense to both prevent and remedy. FACC ¶¶ 359-73. Comcast asserts that Plaintiffs' claims under the Declaratory Judgment Act fail because they are duplicative of other claims alleged, such as negligence and negligence *per se*. 158-2, at 35. But Comcast misunderstands the declaratory relief Plaintiffs seek: a judgment stating that Comcast has a legal duty under statutory and common law to secure Class members' PII, and that Comcast continues to breach this duty. Furthermore, Comcast's argument ignores the fact that Plaintiffs seek separate relief in the form of recovery of damages for injuries caused to date by Defendants' unlawful conduct.

Plaintiffs' declaratory judgment claim is also forward-looking. More than a year after the Data Breach, Defendants have still failed to take the corrective action necessary to meet their obligations to protect Plaintiffs and Class members' PII from unauthorized access, as their data security measures remain inadequate. FACC ¶¶ 388; 511-18. Plaintiffs seek to redress the risk of imminent and future harm created by Defendants' ongoing breach with a judgment that Defendants must remedy their inadequate cybersecurity practices. The Declaratory Judgment Act grants this Court the authority to provide "[f]urther necessary or proper relief based on a declaratory judgment," namely, to enjoin Defendants' negligent conduct by requiring them to employ adequate security protocols consistent with law and industry standards to protect consumers' PII from unauthorized access. The requested declaratory and injunctive relief is necessary to protect Plaintiffs and Class Members from imminent future harm, and courts routinely permit declaratory judgment actions in data breach cases under similar facts. *See, e.g.*, *Clemens v. ExecuPharm, Inc.*, 678 F. Supp. 3d 629, 639 (E.D. Pa. 2023) (dismissal of plaintiff's declaratory judgment claim in a data breach case would be "premature" where "the viability of declaratory relief will depend on the outcome of Plaintiff's surviving substantive claims"); *In re Netgain Tech., LLC*, No. 21-CV-1210 (SRN/LIB), 2022 WL 1810606, at *17 (D. Minn. June 2, 2022) ("Plaintiffs allege that Netgain continues to provide 'inadequate and unreasonable' data security, and that they and the Class 'continue to suffer injury.' This is enough to survive a motion to dismiss.") (citation omitted); *In re Arby's Rest. Group Inc. Litig.*, No. 1:17-CV-0514-AT, 2018 WL 2128441, at *15 (N.D. Ga. Mar. 5, 2018); (same); *In re The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016) (same). This Court should follow these similar data breach actions and deny Comcast's Motion to Dismiss Plaintiffs' claim for declaratory relief.

## IX. PLAINTIFFS ADEQUATELY ALLEGE THE NEED FOR INJUNCTIVE RELIEF.

The allegations of the FACC similarly demonstrate that injunctive relief is warranted. This Court has discretion to grant permanent injunctive relief consistent with the traditional principles of equity. *T.D. Bank N.A. v. Hill*, 928 F.3d 259, 278 (3d Cir. 2019) (internal citation omitted). In order to sufficiently state a claim for a permanent injunction, a plaintiff must allege the following four factors:

> (1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction.

*eBay Inc. v. MercExchange, LLC*, 547 U.S. 388, 391 (2006) (internal citations omitted).

Comcast argues that Plaintiffs have not adequately pleaded a claim for injunctive relief because the requested relief seeks to prevent future injury from a future data breach rather than preventing future injury from *this* Data Breach. ECF No. 158-2, at 36. But this argument assumes that the PII stolen during the Data Breach is now wholly secure and also fails to note that the requested injunctive relief corresponds to Plaintiffs' declaratory judgment claim. *See In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, 2016 WL 2897520 at *4. As set forth *supra*, Plaintiffs allege that Defendants' cybersecurity systems and protocols remain inadequate, placing Plaintiffs and the Class Members at substantial risk of imminent harm in the future, which cannot be adequately addressed by monetary damages. The hardships Class members will endure to prevent further harm from this Data Breach and likely future data breaches if injunctive relief is not granted grossly outweigh the burden placed on Defendants if they are required to implement and maintain adequate security measures. Finally, Plaintiffs have adequately alleged the benefit to

the public at large if Defendants are required to undertake the steps requested by Plaintiffs to prevent future injury.

Courts should not dismiss claims for injunctive relief at an early stage of a case when, as here, such relief could ultimately be appropriate. *See, e.g.*, *In re K-Dur Antitrust Litig.,* 338 F. Supp. 2d 517, 550 (D.N.J. 2004) (noting that where "equitable relief could prove to be an appropriate remedy" the court was "loathe at . . . [the motion to dismiss] stage in the proceedings to curtail its broad equity powers to fashion the most complete relief possible."). Plaintiffs have sufficiently stated a claim for injunctive relief, and Comcast's premature request to dismiss the request for injunctive relief should be denied.

## X. PLAINTIFFS PLEAD CLAIMS AGAINST CLOUD SOFTWARE GROUP.

Citrix claims that Plaintiffs' claims against Cloud Software Group should be dismissed because "the Amended Complaint does not even plead a single cause of action against Cloud [Software Group] at all" and "the Amended Complaint contains no allegations of wrongdoing directed to Cloud Software Group." *See* ECF No. 161, at 34-35. Citrix's argument ignores Plaintiffs' allegations against Cloud Software Group.

As set forth in the FACC, Citrix Systems, Inc., is a subsidiary of Cloud Software Group. FACC ¶ 175. In 2022, Citrix's NetScaler products—the very products involved in the Data Breach—were spun off from Citrix into a different business unit within Cloud Software Group, though Citrix Systems still appeared to maintain some responsibility for maintenance and security of NetScaler products. FACC ¶ 211. As a result of this overlap between Citrix Systems and Cloud Software Group in their management and oversight of NetScaler products, and by extension, their responsibility for the Data Breach, Plaintiffs brought their claims against both entities *jointly* in their FACC. *See* FACC ¶ 1 (stating that the complaint refers to Citrix Systems, Inc. and Cloud Software Group, Inc. collectively as "Citrix"). In cases of such overlap between two closely related

corporate defendants, such pleading is fully permissible. *See In re Riddell Concussion Reduction Litig.*, 77 F. Supp. 3d. 422 at 431-32 (D.N.J. 2015) (rejecting argument that plaintiffs had impermissibly grouped defendants together where "defendants are all owned by the private equity firm . . . are represented by the same counsel, accepted service as a single entity, and all joined in the instant motion to dismiss" and "defendants do not dispute their interrelatedness," noting that "the specific role of each defendant" would be "elucidated through discovery to which Plaintiffs are entitled because the allegations in the Amended Complaint are sufficient to provide notice under Rule 8"); *see also Briskin v. Shopify, Inc.*, --- F.4th. ---, No. 22-15815, 2025 WL 1154075, at *16 (9th Cir. Apr. 21, 2025) (holding that a complaint "provides sufficient information to give [corporate defendants] fair notice of the claims against them," where the complaint "alleges one course of conduct jointly pursued by three closely related corporate defendants"); *Toback v. GNC Holdings*, No. 13-cv-80626, 2013 WL 5206103 at *2 (S.D. Fla. Sept. 13, 2013) (holding that complaint sufficiently put defendants on notice and satisfied Rule 8 despite referring to defendants—GNC Holdings, Inc., GNC Corp, General Nutrition Corporation, and General Nutrition Centers, Inc.—collectively as "GNC" because defendants were interrelated corporate defendants). Plaintiffs' claims against Cloud Software Group should therefore not be dismissed.

## CONCLUSION

The Court should deny Defendants' Motions to Dismiss, and the case should proceed to class certification and trial.

Dated: April 30, 2025

Respectfully submitted,

*/s/ Norman E. Siegel*
Norman E. Siegel
**STUEVE SIEGEL HANSON LLP**
460 Nichols Rd., Ste. 200
Kansas City, MO 64112

*/s/ Gary F. Lynch*
Gary F. Lynch (PA No. 56887)
**LYNCH CARPENTER LLP**
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222

T: (816) 714-7100
siegel@stuevesiegel.com

*Co-Lead Interim Class Counsel*

Charles E. Schaffer (PA No. 76259)
**LEVIN SEDRAN & BERMAN LLP**
510 Walnut Street, Suite 500
Philadelphia, PA 19106
T: (215) 592-1500
cschaffer@lfsblaw.com

*Co-Liaison Counsel*

Ryan J. Clarkson
**CLARKSON LAW FIRM, P.C.**
22525 Pacific Coast Highway
Malibu, CA 90265
T: (213) 788-4050
rclarkson@clarksonlawfirm.com

Amanda G. Fiorilla
**LOWEY DANNENBERG, P.C.**
44 South Broadway, Suite 1100
White Plains, NY 10601
T: (914) 997-0500
afiorilla@lowey.com

Kevin Laukaitis (PA No. 321670)
**LAUKAITIS LAW LLC**
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Matthew L. Lines
**LINES LAW PLLC**
201 Alhambra Circle, Suite 1060
Coral Gables, FL 33134
T: 786-634-4306
lines@lineslaw.com

Amber L. Schubert
**SCHUBERT JONCKHEER &**

Telephone: (412) 322-9243
gary@lcllp.com

*Co-Lead Interim Class Counsel*

James A. Francis (PA No. 77474)
**FRANCIS MAILMAN SOUMILAS, P.C.**
1600 Market Street, Suite 2510
Philadelphia, PA 19103
T: (215) 735-8600
jfrancis@consumerlawfirm.com

*Co-Liaison Counsel*

E. Michelle Drake
**BERGER MONTAGUE PC**
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
T: (612) 594-5933
emdrake@bm.net

Todd S. Garber
**FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP**
One North Broadway, Suite 900
White Plains, New York 10601
T: (914) 298-3281
tgarber@fbfglaw.com

Joe P. Leniski, Jr.
**HERZFELD, SUETHOLZ, GASTEL, LENISKI & WALL, PLLC**
223 Rosa L. Parks Avenue, Suite 300
Nashville, Tennessee 37203
T: (615) 800-6225
joey@hsglawgroup.com

Rosemary M. Rivas
**GIBBS MURA LLP**
1111 Broadway, Suite 2100
Oakland, CA 94607
T: (510) 350-9720
rmr@classlawgroup.com

Diana J. Zinser (PA No. 203449)

**KOLBE LLP**
2001 Union Street, Suite 200
San Francisco, CA 94123
T: (415) 788-4220
aschubert@sjk.law

**SPECTOR ROSEMAN AND KODROFF, P.C.**
2001 Market Street, Suite 3420
Philadelphia, PA 19103
T: (215) 496-0300
dzinser@srkattorneys.com

*Plaintiffs' Executive Committee*